LG Frankfurt a. M.

Urteil vom 18.09.2020, Az. 2-27 O 100/20*

Tenor

Es wird festgestellt, dass die Hauptsache hinsichtlich des Antrags zu 5. b) erledigt ist.

Im Übrigen wird die Klage abgewiesen.

Der Kläger hat die Kosten des Rechtsstreits zu tragen.

Das Urteil ist gegen Sicherheitsleistung In Höhe von 110% des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

Tatbestand

1 Der Kläger macht Unterlassungs-, Schadensersatz und Auskunftsansprüche gegen die Beklagte aufgrund von Verstößen gegen die DS-GVO geltend.

2 Die Beklagte, die ihre Hauptniederlassung in Belgien hat, ist eine Tochtergesellschaft der in den USA ansässigen Mastercard International Inc. Neben Zahlungsdiensten betrieb die Beklagte in Deutschland über ihre Repräsentanz in Frankfurt am Main ein Marketing- und Kundenbindungsprogramm, das Priceless Specials-Programm, Inhaber einer in Deutschland ausgestellten Mastercard konnten sich hierfür unter Angabe persönlicher Daten wie Name, E-Mail-Adresse, Geburtsdatum und Mastercard-Kartennummer im Internet registrieren, um bei Bezahlvorgängen mit ihrer Mastercard Treuepunkte zu sammeln. Diese konnten später gegen Prämien eingelöst werden. Die für den Betrieb des Bonusprogramms erstellte Plattform war physisch und logisch vom Zahlungsnetzwerk der Beklagten getrennt. Der Kläger hat mit der Beklagten einen Vertrag über die Teilnahme an dem Bonusprogramm abgeschlossen.

3 Im April 2017 schloss die Beklagte mit der Brain Behind GmbH (BB GmbH) ein sog. Framework Service Agreement, in dem geregelt war, dass die vertraglichen Verpflichtungen alle am Betrieb der Plattform beteiligten Unternehmen der Brain Behind Gruppe

---

* **Anmerkungen:** Das Urteil wurde von WERNER RI verarbeitet und dabei teils ergänzt (so um die Zwischenüberschriften) und teils gekürzt (z.B. um die Bezeichnungen der Richtlinien und Verordnung); die Seitenzahlen dieses Dokumentes stimmen daher mit den Seitenzahlen des Originalurteils nicht überein. Die Randziffern hingegen sind original.

(BB) treffen sollten. Die Beklagte verpflichtete die BB GmbH zur Einhaltung effektiver Datenschutzstandards, u.a. des Payment Card Industry Datensicherheitsstandards (PCI-DSS-Standards), sowie von Datenschutzmaßnahmen sowie dazu, ihren Auftragsverarbeitern dieselben Pflichten aufzuerlegen. Es wird ergänzend auf die Anlage B 4 verwiesen. Mit der Erstellung der Plattform für das Bonusprogramm war als weiteres Unternehmen der BB die Brain Behind Ltd. (BB Ltd.) beauftragt.

4 Vor Ende der Übergangsperiode zur Umsetzung der DS-GVO Unterzeichnete die „Brainbehind“ einen Datenverarbeitungsvertrag mit der Beklagten und der Mastercard International Inc. Es wird auf die Anlage B 5 verwiesen.

5 Am 21.05.2019 erfolgte ein unbefugter Zugriff auf die Systeme von BB von einer ausländischen IP-Adresse, bei der ein Administratorenpasswort geändert wurde.

6 Am 19. sowie 25.07.2019 erhielt die Beklagte Hinweise auf eine illegale Veröffentlichung von Gutscheincodes aus dem Priceless Specials-Programm im Internet. Die Beklagte und BB gingen dem nach und beauftragten eine IT-Sicherheitsfirma mit der Überprüfung der Firewall. Noch vor Abschluss der Prüfung kam es zu einem nicht genau konkretisierbaren Zeitpunkt zu einem Datenvorfall, bei dem unbekannte Täter die im Rahmen des Bonusprogramms erhobenen Daten von etwa 90.000 Teilnehmern im Internet öffentlich zugänglich machten. Es kamen am 19.08.2019 zwei unterschiedliche Listen in Umlauf, wobei in einer der Listen die vollständige Kartennummer u.a. des Klägers veröffentlicht war. Die Ablaufdaten und Sicherheitscodes (CVC) von Kreditkarten waren nicht betroffen. Technisch erfolgte die Veröffentlichung dergestalt, dass die Daten von einem Träger unter Kontrolle der Beklagten auf einen Webserver kopiert wurden, der diese für die Öffentlichkeit weltweit abrufbar machte.

7 Am 22.08.2019 kontaktierte die Beklagte die betroffenen Kunden, u.a. den Kläger, und warnte vor Missbrauch.

8 Jedenfalls am 29.08.2019 war die Seite des Bonusprogramms aufgrund einer Sicherheitsüberprüfung kurzzeitig erreichbar.

9 Im Nachgang kontaktierte die Beklagte die Betreiber von Internetseiten, auf denen die Daten veröffentlicht waren und ließ die Daten entfernen. Die Beklagte richtete einen Dienst gegen Identitätsdiebstahl ein und überwachte, ob personenbezogene Daten ange-

boten werden. Die betroffenen Karten wurden im System der Beklagten gekennzeichnet, um Missbrauch schneller erkennen zu können. Weiterhin verpflichtete sich die Beklagte, die Kosten eines Austausches der Karte infolge des Vorfalls zu übernehmen. Hinweise auf Datenmissbrauch gab es bisher nicht.

10 Unter dem 14.10.2019 forderte der Kläger die Beklagte unter Fristsetzung zur Abgabe einer strafbewehrten Unterlassungserklärung auf und machte Schadensersatz- und Auskunftsansprüche geltend.

11 Inzwischen speichert BB die Daten nicht mehr, dies tut die Beklagte selbst. Das Bonusprogramm wurde zudem beendet, die Beklagte ließ den Teilnehmern am 04.06.2020 eine Kündigung zukommen.

12 Der Kläger ist der Ansicht, die Beklagte habe durch Datenveröffentlichung gegen die DS-GVO verstoßen. Er behauptet, die Beklagte bzw. BB hätten technische und organisatorische Sicherheitsmaßnahmen missachtet. Der Kläger bestreitet, dass BB vor der Auftragsvergabe einen aufwändigen Auswahlprozess hinsichtlich der Gewährleistung datenschutzrechtlicher Vorgaben durchlaufen habe und Zertifikate für die Einhaltung von ISO/IEC 27001 und PCI-DSS vorgelegt habe. Weder im Februar 2018 noch im weiteren Verlauf sei die Beklagte ihren Überprüfungspflichten nach Art. 25, Art. 32 DS-GVO nachgekommen um sicherzustellen, dass die vertraglich festgelegten Maßnahmen den risikoadäquaten Sicherheitsstandards genügten. Die Beklagte bzw. das von ihr beauftragte Unternehmen habe PCI-DSS-Standards verletzt, weil die Primary Account Number (PAN, d.h. die Kreditkartennummer) ohne die Verwendung von Hashes gespeichert worden sei. Die Beklagte habe ihrem Dienstleister die Klardaten übermittelt bzw. ihn nicht verpflichtet, nach eigener Erhebung der Daten Hashes einzusetzen, Die Verwendung einer anderen starken Kryptografie sei ebenfalls nicht erfolgt. Das Datenleck sei dadurch entstanden, dass ein Angreifer über ein Administratorenkonto mit noch immer voreingestelltem Initialpasswort auf die BB-Umgebung habe zugreifen können, Ein weiterer Verstoß der Beklagten gegen die DS-GVO liege darin, dass die Plattform nach dem 19.08.2019 noch zugänglich gewesen sei und sich am 29.08.2019 jedermann wieder habe einloggen können. Zu beanstanden sei auch, dass es weder mit der BB GmbH noch mit der BB Ltd. eine wirksame Vereinbarung nach Art. 28 DS-GVO gegeben habe.

13 Dass zwischen der Beklagten und der Mastercard International Inc, eine Vereinbarung nach Art. 26 DS-GVO fehle, obwohl beide ausweislich des vorgelegten Datenverarbeitungsvertrages Zwecke und Mittel der Verarbeitung durch die BB festgelegt hätten, verstoße gleichfalls gegen die DS-GVO. Für eine Datenverarbeitung durch die Mastercard International Inc, habe es zudem an einer Rechtsgrundlage gefehlt, ebenso an einer geeigneten Garantie nach Art. 46 DS-GVO. Der Link zu den Mastercard Binding Corporate Rules sei nicht ausreichend, weil die Internetpräsenz veränderlich sei und außerhalb der Vertragsurkunde liege.

14 Es bestehe – nach wie vor – ein erhebliches Missbrauchspotential, insbesondere im Hinblick auf einen Identitätsdiebstahl.

15 Der Kläger hat beantragt,

1. die Beklagte zu verurteilen,

   es bei Meidung eines Ordnungsgeldes von bis zu 250.000,-- €, ersatzweise Ordnungshaft zu vollziehen an den Mitgliedern des Verwaltungsrats, oder Ordnungshaft von bis zu sechs Monaten zu vollziehen an den Mitgliedern des Verwaltungsrates,

   zu unterlassen, personenbezogene Daten des Klägers zu verarbeiten und diese zu veröffentlichen oder veröffentlichen zu lassen, wie geschehen bei der Verarbeitung von zur Durchführung des Bonusprogramms „Priceless Specials“ eingesetzten Vertragsdaten des Klägers anlässlich dessen Teilnahme an dem Bonusprogramm der Beklagten im Jahr 2019;

2. Hilfsweise zum Antrag zu 1.:

   die Beklagte zu verurteilen,

   es bei Meldung eines Ordnungsgeldes von bis zu 250.000,-- €, ersatzweise Ordnungshaft zu vollziehen an den Mitgliedern des Verwaltungsrats, oder Ordnungshaft von bis zu sechs Monaten zu vollziehen an den Mitgliedern des Verwaltungsrates,

zu unterlassen, personenbezogene Daten des Klägers zu verarbeiten, ohne risikoadäquate Maßnahmen zum Schutz der Daten gegen ihre nicht durch einen gesetzlichen oder vertraglichen Erlaubnistatbestand gedeckte Veröffentlichung zu ergreifen, wie geschehen bei der Verarbeitung von zur Durchführung des Bonusprogramms „Priceless Specials“ eingesetzten Vertragsdaten des Klägers anlässlich dessen Teilnahme an dem Bonusprogramm der Beklagten im Jahr 2019;

3. die Beklagte zu verurteilen, an den Kläger einen Betrag in Höhe von 8:400,-- € nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 18.10.2019 auf 2.000,-- € und weitere Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz ab Rechtshängigkeit auf 6.400,-- € zu zahlen.

4. festzustellen, dass die Beklagte verpflichtet ist, dem Kläger jeden Schaden zu ersetzen, der diesem wegen der Verarbeitung seiner personenbezogenen Daten, die von der Beklagten zwecks Durchführung ihres Bonusprogramms mit dem Namen „Priceless Specials“ verarbeitet wurden, gern. Antrag zu 1., hilfsweise zu 2. entstanden ist und künftig entsteht;

5. die Beklagte zu verurteilen, dem Kläger im Rahmen einer geordneten Aufstellung Auskunft zu erteilen,

   a. über Dauer und Umfang der Antrag zu 1., hilfsweise Antrag zu 2, genannten Rechtsverletzung sowie

   b. über die Identität eingesetzter Dienstleister bei der zugrunde liegenden Verarbeitungstätigkeit;

6. die Beklagte zu verurteilen, an den Kläger einen Betrag von 1.029,35 € zzgl. Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 18.10.2019 zu zahlen.

16 Er beantragt zuletzt unter Aufrechterhaltung der weiteren Anträge mit dem Antrag zu 5.b),

festzustellen, dass die Hauptsache hinsichtlich des Antrags erledigt ist, die Beklagte zu verurteilen, dem Kläger im Rahmen einer geordneten Aufstellung Auskunft zu erteilen, über die Identität eingesetzter Dienstleister bei der zugrunde liegenden Verarbeitungstätigkeit.

17 Die Beklagte beantragt,

die Klage abzuweisen.

18 Die Beklagte ist der Auffassung die Anträge zu 1. und 2. seien nicht hinreichend bestimmt genug. Dessen ungeachtet bestehe auch in der Sache kein Unterlassungsanspruch gegen sie, u.a. fehle es an einer Wiederholungsgefahr, Weiter sei der Beklagten kein Verstoß gegen die DS-GVO vorzuwerfen. Sie behauptet, die veröffentlichten Daten seien von BB für das Bonusprogramm erhoben und auch nur dort gespeichert worden. Die Beklagte hätte den Vorfall nicht verhindern können, es seien alle technischen und organisatorischen Maßnahmen getroffen worden, um ein hinreichendes Schutzniveau zu schaffen. Auch in der Folge sei der Beklagten kein Verstoß gegen die DS-GVO vorzuwerfen. Nach dem Datenvorfall am 19.08.2019 sei die Priceless Specials-Webseite taggleich deaktiviert worden und lediglich am 29.08.2019 unter Sicherheitsvorkehrungen zu einer Sicherheitsprüfung aktiviert worden.

19 Wegen des weiteren Vorbringens der Parteien wird auf die gewechselten Schriftsätze nebst Anlagen verwiesen.

Entscheidungsgründe:

20 Die bis auf den Hilfsantrag zulässige Klage ist lediglich mit dem Antrag zu 5.b. begründet.

Örtliche Zuständigkeit

21 Das angerufene Gericht ist international und örtlich zuständig. Die internationale Zuständigkeit ergibt sich aus Art. 79 Abs. 2 DS-GVO und aus Art. 7 Nr. 5 EuGVVO (vgl. MüKo, ZPO, 5. Aufl., Brüssel Ia-VO, Art. 7, Rn. 74). Die Beklagte hat zwar ihren Sitz in Belgien. Sie kann jedoch vorliegend in Deutschland, konkret in Frankfurt am Main verklagt werden, weil es um eine Streitigkeit aus dem Betrieb der Repräsentanz geht, die sich hier befindet.

Antrag zu 1. (Kein Unterlassungsanspruch hinsichtlich der Verarbeitung und der Veröffentlichung)

22 Der Kläger hat gegen die Beklagte **keinen Anspruch** nach §§ 1004 Abs. 1, 823 Abs. 1 BGB analog darauf, es zu unterlassen, personenbezogene Daten des Klägers zu verarbeiten und diese zu veröffentlichen oder veröffentlichen zu lassen, wie geschehen bei der Verarbeitung von zur Durchführung des Bonusprogramms „Priceless Specials“ eingesetzten Vertragsdaten des Klägers anlässlich dessen Teilnahme an dem Bonusprogramm der Beklagten im Jahr 2019.

23 Der Antrag ist **zulässig**, insbesondere hinreichend bestimmt, § 253 Abs. 2 Nr. 2 ZPO. Aus dem Wortlaut ergibt sich, dass sich der Kläger sowohl gegen eine Verarbeitung als auch gegen eine Veröffentlichung seiner Daten wendet.

24 Der Antrag ist **jedoch unbegründet**. Zu einer Unterlassung der Datenverarbeitung ist die Beklagte nicht verpflichtet, solange die mit der Teilnahme am Bonusprogramm erteilte Einwilligung des Klägers in die Datenverarbeitung fortbesteht. Soweit der Kläger die Unterlassung der (unzulässigen) Veröffentlichung seiner Daten begehrt, fehlt es an einer Wiederholungsgefahr. Die Wiederholungsgefahr ist materielle Anspruchsvoraussetzung für den Unterlassungsanspruch. Sie ist die auf Tatsachen gegründete objektive ernsthafte Besorgnis weiterer Störungen. Eine vorangegangene rechtswidrige Beeinträchtigung wie sie vorliegend unstreitig erfolgt ist, begründet grundsätzlich eine tatsächliche Vermutung für das Bestehen einer Wiederholungsgefahr, an deren Widerlegung durch den Störer hohe Anforderungen zu stellen sind (siehe BGH, NJW 2004, 3701). Diese hohen Anforderungen sind durch die Beklagte erfüllt. Denn zum einen kann eine Vermutung nur so lange gelten, wie der ihr zugrundeliegende Sachverhalt unverändert fortbesteht (OLG Schleswig Urteil vom 28.02.2012, Az. 11 U 64/10, BeckRS 2013, 3123). Der Sachverhalt hat sich jedoch hier maßgeblich geändert. Die BB, bei der es zu dem Datenleck gekommen war, verwaltet die Daten des Klägers nicht mehr, dies hat zwischenzeitlich die Beklagte selbst übernommen. Dass bei der BB aufgrund mangelnder Sicherheitsvorkehrungen Daten abgegriffen werden können, ist daher ausgeschlossen. Die Seite des Bonusprogramms ist ferner zwischenzeitlich offline und das Programm beendet; die Beklagte hat ihren Kunden – also auch dem Kläger – eine Kündigung zukommen lassen. Die Internetseite als Einfallstor für unberechtigte Zugriffe ist nicht mehr vorhanden. Zum anderen kann eine Widerlegung der Widerholungsgefahr

ausnahmsweise angenommen werden, wenn der Eingriff durch eine einmalige Sondersituation veranlasst gewesen ist (BGH, Urteil vom 14.11.2017, Az. VI ZR 534/15, Rn. 17, juris). Ein etwaiges kriminelles und unvorhersehbares Verhalten eines externen oder internen Dritten begründet ohne Zweifel eine derartige Sondersituation. Schließlich ist davon auszugehen, dass ein Rechtsschutzinteresse des Klägers an der begehrten Unterlassung deswegen nicht gegeben sein dürfte, weil die Beklagte an dem Schutz seiner Daten bereits aus ökonomischen Gründen ein ebenso hohes Interesse hat wie der Kläger selbst.

25 Weitere Anspruchsgrundlagen, die keine Wiederholungsgefahr voraussetzen, sind nicht ersichtlich, Insbesondere kann der Kläger seinen Anspruch nicht aus Art. 82 DS-GVO oder § 280 Abs. 1 BGB herleiten, da beide Normen auf Schadensersatz als Rechtsfolge gerichtet sind.

Antrag zu 2./Hilfsantrag (Keine Unterlassungsanspruch hinsichtlich der Datenverarbeitung ohne risikoadäquate Maßnahmen / TOMs)

26 Der Kläger hat gegen die Beklagte **keinen Anspruch** darauf, es zu unterlassen, personenbezogene Daten des Klägers zu verarbeiten, ohne risikoadäquate Maßnahmen zum Schutz der Daten gegen ihre nicht durch einen gesetzlichen oder vertraglichen Erlaubnistatbestand gedeckte Veröffentlichung zu ergreifen, wie geschehen bei der Verarbeitung von zur Durchführung des Bonusprogramms „Priceless Specials“ eingesetzten Vertragsdaten des Klägers anlässlich dessen Teilnahme an dem Bonusprogramm der Beklagten im Jahr 2019.

27 Der **Antrag genügt nicht den Anforderungen** des § 253 Abs. 2 Nr. 2 ZPO, da er zu unbestimmt ist. Er lässt weder für die Rechtsverteidigung der Beklagten noch für die Vollstreckung erkennen, worauf sich das Verbot erstreckt. Weiche Maßnahmen „risikoadäquat“ sind und daher von der Beklagten zu ergreifen wären, damit die Verarbeitung der Daten des Klägers stattfinden darf, lässt der Antrag offen, Dies lässt sich auch nicht anderweitig etwa durch Auslegung bestimmen. Eines gesonderten richterlichen Hinweises nach § 139 ZPO bedurfte es nicht, nachdem die Beklagte auf die mangelnde Bestimmtheit des Antrags in der Klageerwiderung ausdrücklich hingewiesen hatte (Bl. 89 d.A.).

28 Darüber hinaus ist auch der hilfsweise gestellte Unterlassungsantrag unbegründet, da es aus den oben genannten Gründen an einer Wiederholungsgefahr fehlt.

Antrag zu 3. (Kein Anspruch auf Zahlung von 8.400,-- €)

29 Ein Anspruch des Klägers gegen die Beklagte auf Zahlung von 8.400,-- € nach Art. 82 DS-GVO besteht nicht.

30 Nach Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen. Dem Kläger ist zwar unstreitig bisher kein materieller Schaden entstanden, wohl aber ein immaterieller Schaden. Dieser liegt darin, dass seine personenbezogenen Daten Dritten ohne sein Einverständnis zugänglich wurden. Die Kompensation einer solchen öffentlichen „Bloßstellung“ fällt unter Art. 82 Abs. 1 DS-GVO (Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 82 Rn. 13; Sydow, DS-GVO, 2. Aufl., Art. 82 Rn. 6). Die Beklagte ist auch tauglicher Anspruchsgegner. Sie war Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO, da sie über die Zwecke und Mittel der – unstreitig – stattgefundenen Verarbeitung der Daten des Klägers entschied.

31 Der Schaden muss jedoch wegen eines Verstoßes gegen die DS-GVO entstanden sein. Es muss also ein Verstoß gegen die DS-GVO und dessen Kausalität für den Schaden festgestellt werden. Ein Rechtsgut der betroffenen Person muss infolge der Verletzung einer Norm der DS-GVO im Vergleich zum status quo ante nachteilig verändert worden sein (Ehmann/Selmayr, DS-GVO 2. Aufl. Art. 82 Rn. 11).

32 Die Veröffentlichung der Daten, für die der Kläger einen **Schadensersatz von 2.000,-- €** geltend macht, stellt an sich keinen Verstoß der Beklagten gegen die DS-GVO dar. Die Veröffentlichung könnte nur dann als Verstoß gegen Art. 5 Abs. 1 lit. a) oder lit. f) DS-GVO eingeordnet werden, wenn die Beklagte bzw. BB sie unberechtigt vorgenommen hätte. Dies lässt sich aber nicht feststellen und wird auch von dem Kläger nicht konkret vorgetragen. Der Kläger ist jedoch für den Verstoß gegen die DS-GVO darlegungs- und beweisbelastet; erst hinsichtlich der Verantwortlichkeit für den Verstoß sieht Art. 82 Abs. 3 DS-GVO eine Vermutung zu Lasten des Anspruchsgegners vor. Hat die Beklagte bzw. BB die Veröffentlichung nicht selbst vorgenommen, so kann sie lediglich die Folge einer Verletzung der Pflichten aus der DS-GVO durch die Beklagte bzw. BB sein, nicht aber der Verstoß an sich.

33 Der Schadensersatzanspruch folgt weiter nicht daraus, dass die Beklagte die BB GmbH nicht nach Art. 28 Abs. 1 DS-GVO ordnungsgemäß ausgewählt oder überwacht hat. Dass dies nicht geschehen ist, lässt sich nach dem Sach- und Streitstand schon nicht

feststellen. Ein entsprechendes Beweisangebot des Klägers fehlt, ebenso entsprechende Indizien. Insbesondere kann der Kläger sich nicht darauf berufen, es sei offensichtlich, dass die BB GmbH ihr auferlegte Sicherheitsvorkehrungen nicht einhalten könne, weil es sich bei dem Firmensitz um ein Einfamilienhaus in einer Wohnsiedlung handele. Dass sich der Firmensitz dort befindet, sagt nichts darüber aus, wo die Datenverarbeitung erfolgt. Darüber hinaus lässt sich die Kausalität eines etwaigen Verstoßes gegen Pflichten der Beklagten aus der DS-GVO für den Datenvorfall und damit für den Schaden des Klägers nicht feststellen. Denn letztlich ist - auch nach dem zuletzt gehaltenen und bestrittenen Vortrag des Klägers hinsichtlich des nicht geänderten Initialpassworts - letztlich unklar geblieben, wodurch das Datenleck verursacht wurde. Dass es durch ein anderes Auswahlverfahren, andere Sicherheitsvorkehrungen oder andere Überwachungen verhindert hätte werden können, bleibt danach Spekulation, Hinzu kommt, dass ein werkseitig individuell voreingestelltes Passwort im Ausgangspunkt nicht weniger sicher als ein vom Nutzer persönlich eingestelltes Passwort sein muss (BGH, Urteil vom 24.11.2016, Az. I ZR 220/15, Rn. 16, juris).

34 Soweit der Kläger seinen **Anspruch in Höhe von 700,-- €** darauf stützt, dass seine Daten nach dem 19.08.2019 noch verfügbar gewesen seien und jedenfalls während eines IT-Checks am 29.08.2019 jedermann habe auf sie zugreifen können, vermag dies ebenfalls keinen Schadensersatzanspruch zu begründen. Es kann dahinstehen, ob überhaupt ein Verstoß gegen die DS-GVO vorliegt. Denn jedenfalls ist dem Kläger kein Schaden entstanden. Der Kläger behauptet nicht, dass nach dem 19.08.2019 seine Daten nochmals veröffentlicht worden seien oder sie von Unbefugten etwa während des Checks tatsächlich zur Kenntnis genommen worden wären. Dann aber steht dem Kläger kein Schadensersatzanspruch zu. Denn nicht jede Datenschutzrechtverletzung in Form einer nicht (vollständig) rechtskonformen Datenverarbeitung ist automatisch ein ersatzfähiger Schaden (vgl. etwa Wybitul, NJW 2019, 3265 m.w.N.), Vielmehr muss die Verletzungshandlung auch zu einer konkreten Verletzung von Persönlichkeitsrechten der betroffenen Person geführt haben (Wybitul, a.a.O.). Eine weite Auslegung des Schadensbegriffs nach Art. 82 DS-GVO, nach dem mit jedem Verstoß ein Schaden begründet wird (sowohl Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 82 Rn. 13), widerspricht der Systematik des deutschen Rechts. Die mitgliedsstaatlichen Gerichte sind zu einem überkompensatorischen Strafschadensersatz grundsätzlich nicht verpflichtet; nach dem

Äquivalenzgrundsatz wäre ein solcher nur dann erforderlich, wenn die mitgliedstaatliche Rechtsordnung allgemein Strafschadensersatz vorsieht (Wytibul, a.a.O.). Das ist jedoch in Deutschland nicht der Fall.

35 Aus dem identischen Grund steht dem Kläger kein **Anspruch in Höhe von 700,-- €** wegen Änderung des Administratorenpasswortes im Mai 2019 zu.

36 Ferner kann der Kläger nicht damit gehört werden, die Beklagte habe gegen Art. 28 DS-GVO verstoßen, weil ein Vertrag nach dieser Norm mit BB fehle. Ein **Schadensersatzanspruch in Höhe von 800,-- €** besteht insofern nicht. Die Beklagte hat einen Datenverarbeitungsvertrag mit der BB GmbH geschlossen. Zwar ist in dem Vertrag kein Rechtsformzusatz für die dort bezeichnete „Brainbehind" genannt. Allerdings ergibt sich aus den weiteren zu ihr genannten Daten, dass es sich um die GmbH handelte. Dass der Vertrag nicht von sämtlichen Parteien unterzeichnet wurde, ist unerheblich. Nach Art. 28 Abs. 9 DS-GVO bedarf es einer schriftlichen Abfassung, auch in elektronischem Format. Danach ist keine Unterzeichnung erforderlich (vgl. Ehmann/Semayr, DS-GVO, 2. Aufl., Art. 28 Rn. 12); es genügt die Abfassung in Textform nach § 126b BGB. Diesem Erfordernis genügt der Vertrag. Ferner ist nicht ersichtlich, dass der Vertrag den Anforderungen des Art. 28 DS-GVO nicht genügen würde. Dass mit der BB Ltd. kein gesonderter Vertrag geschlossen wurde, ist ebenfalls unschädlich. Denn es war vertraglich unter Ziffer 7 des Vertrages geregelt, dass die BB GmbH bei einem Einsatz von Unterverarbeitern diesen gegenüber mindestens dieselben Datenschutzverpflichtungen festzulegen hatte, wie sie der Vertrag zwischen der Beklagten und der BB GmbH vorsah. Dies entspricht Art. 28 Abs. 4 DS-GVO. Auch der hierfür geltend gemachte **Anspruch in Höhe von 1.000,-- €** besteht nicht.

37 Auf die unterlassene Verwendung von Hashes kann der Kläger gleichfalls keinen Schadensersatzanspruch stützen, weil ein Verstoß gegen die DS-GVO nicht vorliegt. Bei der Verarbeitung der personenbezogenen Daten muss eine angemessene Sicherheit gewährleistet sein, Art. 5 Abs. 1 lit. f) DS-GVO, Dies erfordert geeignete technische und organisatorische Maßnahmen zum Schutz vor unbefugter und unrechtmäßiger Verarbeitung, wobei die Anforderungen in Art. 32 DS-GVO festgelegt werden. Art. 32 Abs. 1 lit. a) DS-GVO erwähnt zwar Verschlüsselung als technisches Maßnahme, fordert die Anwendung von Hashes aber gerade nicht. Selbiges gilt für die PCC-DSS-Standards. Für seine Behauptung, es sei auch keine anderweitige Kryptografie erfolgt bietet der Kläger keinen Beweis an.

38 Der Kläger hat gegen die Beklagte keinen Anspruch auf **Schadensersatz in Höhe von 1.000,-- €**, weil Daten gegenüber der Mastercard International inc. ohne Rechtsgrundlage zugänglich gemacht worden wären. Dass der Mastercard International Inc. im Rahmen des Priceless Specials Programms erhobene Daten von Kunden preisgegeben wurden, trägt der Kläger schon nicht substantiiert vor. Erst recht gilt dies für seine konkreten Daten. Dass die Mastercard International Inc. an der Datenverarbeitung beteiligt war, ist aufgrund des als Anlage B 5 vorgelegten Vertrages auch keineswegs zwingend. Dies gilt auch dann, wenn die Mastercard Inc. gemeinsame Verantwortliche nach Art. 26 DS-GVO gewesen sein sollte. Denn der Verantwortliche hat die Entscheidungsgewalt über Zweck und Mittel der Verarbeitung; diese kann auch ausgeübt werden, ohne dass der Verantwortliche selbst an der Durchführung der Verarbeitung beteiligt ist (Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 4 Rn. 36). Es fehlt danach an einem Schaden des Klägers.

39 Die Behauptung des Klägers, es fehle an einer Vereinbarung zur gemeinsamen Verantwortlichkeit, was ihm zusätzlich nicht mitgeteilt worden sei, rechtfertigt keinen **Schadensersatzanspruch in Höhe von insgesamt 1.200,-- €**. Erneut fehlt es an einem Schaden des Klägers, weil nicht ersichtlich ist, dass seine Daten der Mastercard International Inc. überhaupt zugänglich gemacht wurden. Überdies regelt Art. 26 DS-GVO lediglich, dass bei zwei oder mehr Verantwortlichen festzulegen ist, wer welche Verpflichtung gemäß der Verordnung erfüllt. Wo der Schaden des Klägers liegen soll, wenn dies nicht geschehen ist und er nicht informiert wurde, ist nicht ersichtlich. Dies gilt insbesondere vor dem Hintergrund des Art. 26 Abs. 3 DS-GVO. Schließlich kann der Kläger keinen **Schadensersatz in Höhe von 1.000,-- €** deswegen gegen die Beklagte geltend machen, weil keine ausreichende Vereinbarung von Binding Corporate Rules für Zugriffsmöglichkeiten durch ein US-Unternehmen auf Daten erfolgt sei. Erneut ist schon eine Beeinträchtigung des Klägers nicht feststellbar (s.o.). Ungeachtet dessen lag für die Mastercard International Inc. eine geeignete Garantie in Form von verbindlichen internen Datenschutzvorschriften nach Art. 46 Abs. 1, Abs. 2b), Art. 47 DS-GVO vor. Aus dem Datenverarbeitungsvertrag ergibt sich, dass durch die zuständige Aufsichtsbehörde genehmigte Binding Corporate Rules existierten, was ausreichend ist. Für seinen das in Abrede stellenden Vortrag ist der Kläger beweisfällig geblieben.

40 Für andere deliktische Ansprüche besteht eine Sperrwirkung der DS-GVO (Sydow, DS-GVO, 2. Aufl., Art. 82 Rn.27).

41 Ein Anspruch aus § 280 Abs. 1 BGB besteht gleichfalls nicht, weil sich nach den obigen Ausführungen nicht feststellen lässt, dass die Beklagte eine Vertragspflichtverletzung begangen hat, die kausal zu einem Schaden, nämlich der Beeinträchtigung des Allgemeinen Persönlichkeitsrechts des Klägers, geführt hat.

Antrag zu 4. (Keine Feststellung der Schadensersatzverpflichtung dem Grunde nach)

42 Ein Anspruch des Klägers gegen die Beklagte auf Feststellung, dass die Beklagte verpflichtet ist, dem Kläger jeden Schaden zu ersetzen, der diesem wegen der Verarbeitung seiner personenbezogenen Daten, die von der Beklagten zwecks Durchführung ihres Bonusprogramms mit dem Namen „Priceless Specials“ im Jahr 2019 verarbeitet wurden, entstanden ist und künftig entsteht, besteht nicht.

43 Ein vertraglicher oder deliktischer Anspruch des Klägers gegen die Beklagte, der die Feststellung rechtfertigen würde, ist mit den Ausführungen unter 3. nicht gegeben.

Antrag zu 5.a. (Kein Auskunftsanspruch)

44 Ein Anspruch des Klägers gegen die Beklagte gemäß § 242 BGB auf Auskunftserteilung über Dauer und Umfang von Rechtsverletzungen bei der Datenverarbeitung durch die Beklagte besteht nicht.

45 Da kein Leistungsanspruch des Klägers gegen die Beklagte gegeben ist, kommt es für dessen Höhe auch nicht wie von dem Kläger geltend gemacht auf Dauer und Umfang der Rechtsverletzung an.

Antrag zu 5.b. (Auskunft über die Identität eingesetzter Dienstleister)

46 Der Kläger hat einen Anspruch auf Feststellung, dass sich die Hauptsache hinsichtlich des Antrags zu 5.b) erledigt hat.

47 Der Antrag des Klägers gegen die Beklagte auf **Auskunft über die Identität eingesetzter Dienstleister** bei der Verarbeitung seiner Daten im Rahmen des Bonusprogramms „Priceless Specials“ **war ursprünglich zulässig und begründet**. Der Anspruch resultierte aus Art. 15 Abs. 1c) DS-GVO. Hiernach hat die betroffene Person, wenn sie betreffende personenbezogene Daten verarbeitet wurden gegen den Verantwortlichen An-

spruch auf Information über die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt wurden oder noch offengelegt werden. Betroffene Person ist vorliegend der Kläger, Verantwortliche bzgl. der Verarbeitung der Daten des Klägers im Sinne des Art. 4 Nr. 7 DS-GVO die Beklagte (s.o.). Der Auftragsverarbeiter ist Empfänger im Sinne von Art. 15 Abs. 1c), Abs. 4 Nr. 9 DS-GVO (vgl. Lins/Raschauer, WM 2018, 2345), so dass der Kläger entsprechend auch verlangen konnte, dass ihm die Identität des bei der Datenverarbeitung eingesetzten Dienstleisters mitgeteilt werde.

48 Die Klage ist nachträglich unbegründet geworden, weil die Beklagte die Auskunft über die Identität der Auftragsverarbeiter im Laufe des Verfahrens mitgeteilt hat.

Antrag zu 6. (Kein Anspruch auf Abmahnkosten)

49 Ein Anspruch des Klägers auf Zahlung der Abmahnkosten von 1.029,35 € gegen die Beklagte aus Art. 82 Abs. 1 DS-GVO, aus § 280 Abs. 1 BGB oder aus § 823 Abs. 1 BGB besteht nicht, da die vorgerichtlichen Rechtsanwaltskosten das Schicksal der Hauptforderung teilen.