

ZH_HANDELSGERICHT HE190100 vom 21. Mai 2019

Zh Handelsgericht, 2019-05-21, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/zh_handelsgericht_HE190100

FR: ZH_HANDELSGERICHT HE190100 du 21 mai 2019

IT: ZH_HANDELSGERICHT HE190100 del 21 maggio 2019

Erwägungen

E. 5

Rechtsschutzinteresse

E. 5.1

Das Rechtsschutzinteresse ist eine weitere Prozessvoraussetzung, die das Gericht von Amtes wegen zu prüfen hat (Art. 59 Abs. 2 lit. a i.V.m. Art. 60 ZPO). Bei Unterlassungsklagen ist das Rechtsschutzinteresse gegeben, wenn die wider- rechtliche Handlung, auf welche das Begehren gerichtet ist, unmittelbar droht, d.h., wenn das Verhalten der Beklagten die künftige Rechtsverletzung ernsthaft befürchten lässt (ZÜRCHER in: Sutter-Somm/Hasenböhler/Leuenberger [Hrsg.], Kommentar zur Schweizerischen Zivilprozessordnung (ZPO), 3. Aufl., Zürich 2016, Art. 59 N 13, m.w.H.).

- 9 -

E. 5.2

Das Rechtsschutzinteresse der Klägerin 1 wird nicht bestritten. Die Beklag- te behauptet jedoch, die ohnehin in anonymisierter Weise zu übermittelnden Da- ten seien von vornherein nicht dem Kläger 2 zuzuordnen. Daher habe er kein Rechtsschutzinteresse, die geplante Datenübermittlung zu verhindern, weshalb auf sein Gesuch nicht einzutreten sei (act. 11 Rz 15 ff.). Wie bereits oben erläutert, handelt es sich bei der drohenden Persönlichkeitsver- letzung um eine doppelrelevante Tatsache, welche sowohl für die Zulässigkeit als auch die Begründetheit der Klage bedeutsam ist. Sie wird nur bei der Prüfung der Begründetheit untersucht, sofern der klägerische Parteivortrag nicht von vornhe- rein als fadenscheinig erscheint. Sollte dann keine unmittelbare Drohung einer Rechtsverletzung festgestellt werden, ist auf die Klage einzutreten, diese aber als unbegründet abzuweisen (BOPP/BESSENICH in: Sutter- Somm/Hasenböhler/Leuenberger [Hrsg.], Kommentar zur Schweizerischen Zivil- prozessordnung (ZPO), 3. Aufl., Zürich 2016, Art. 84 N 9). Vorliegend führt die Beklagte selbst aus, der Kläger 2 sei bis 2010 der wirtschaft- lich Berechtigte der streitgegenständlichen Konten gewesen (act. 11 Rz 49 ff.). Zudem wird der Kläger 2 im an das DoJ zu übermittelnde Factsheet als "beneficial owner 1" bezeichnet (act. 3/11/2; siehe unten unter Ziffer 6.3.3.2). Daraus ergibt sich ohne Weiteres, dass die bekanntzugebenden Daten einen Bezug zum Klä- ger 2 haben, weshalb sein behauptetes Rechtsschutzinteresse nicht als inkohä- rent bezeichnet werden kann.

E. 5.3

Im Rahmen des Rechtsschutzinteresses bleibt jedoch das Begehren der Kläger zu prüfen, wonach die streitgegenständliche Datenbekanntgabe nicht nur an das DoJ sondern allgemein an US-Behörden und ins Ausland zu untersagen sei. Ein hinreichendes schutzwürdiges Interesse ist bei einer Unterlassungsklage wie erwähnt nur dann gegeben,

wenn eine künftige Persönlichkeitsverletzung ernsthaft und mit einer gewissen Unmittelbarkeit droht (BGE 124 III 72, E. 2a). In welcher Intensität eine einschlägige Gefahr vorhanden sein muss, um einen Unterlassungsanspruch bejahen zu können, ist eine Rechtsfrage. Die tatsächlichen

- 10 - Gegebenheiten, aus denen sich eine Gefahr der dargelegten Art ergeben soll, sind von den Klägern nachzuweisen (Urteile des Bundesgerichts 4A_250/2018 vom 1. Oktober 2018, E. 3.2, 5A_228/2009 vom 8. Juli 2009, E. 4.1). In seinem Urteil 4A_250/2018 vom 1. Oktober 2018 erwog das Bundesgericht in einem ähnlich gelagerten Fall, bei welchem ein Verbot zur Datenherausgabe neben dem DoJ auch gegenüber dem Internal Revenue Service (IRS) beantragt wurde, dass zur Bejahung eines schutzwürdigen Interesses an einem Verbot zur Datenherausgabe vom Kläger dargetan werden müsse, dass eine Datenherausgabe auch vom IRS verlangt worden sei oder ein entsprechendes Begehren bevorstehe und dass der Adressat eines solchen Begehrens – mangels Verbot – diesem auch stattgeben würde. Mangels konkreter Anhaltspunkte verneinte das Bundesgericht ein schutzwürdiges Interesse hinsichtlich einer Datenherausgabe an den IRS und hielt fest, dass die Vorinstanz diesbezüglich auf die Klage nicht hätte eintreten dürfen (E. 3.2). Nicht anders verhält es sich bei der vorliegend in Frage stehenden Datenübermittlung, ist doch weder dargetan worden noch ersichtlich, dass eine Datenbekanntgabe auch "ins Ausland" oder an andere US-Behörden als das DoJ drohen würde. An einem allgemeinen Verbot zur Datenübermittlung besteht somit kein schutzwürdiges Interesse. Demnach ist auf die Klage insoweit nicht einzutreten, als sich das Verbot zur Datenübermittlung auf andere US-Behörden als das DoJ oder das Ausland allgemein bezieht. Im Übrigen ist auf die Klage einzutreten.

E. 6

Würdigung

E. 6.1

Anwendbares Recht Vorliegend ist Schweizer Recht anzuwenden, was von den Parteien auch nicht bestritten wird. Das klägerische Gesuch stützt sich insbesondere auf Art. 6 DSGVO. Diese Bestimmung gilt gestützt auf Art. 18 IPRG für alle von der Schweiz aus gelieferten Daten (lois d'application immédiate; vgl. DASSER, in: BSK-DSG, 3. Aufl., Basel 2013, N 49 zu Art. 139).

- 11 -

E. 6.2

Voraussetzungen zum Erlass vorsorglicher Massnahmen Das Gericht trifft die notwendigen vorsorglichen Massnahmen, wenn die gesuchstellende Partei glaubhaft macht, dass ein ihr zustehender Anspruch verletzt ist oder eine Verletzung zu befürchten ist und dass ihr aus der Verletzung ein nicht leicht wieder gutmachender Nachteil droht (Art. 261 Abs. 1 ZPO). Zu den Voraussetzungen zählen insbesondere das Vorliegen eines Verfügungsanspruchs und eines Verfügungsgrundes (BSK-SPRECHER, 3. Aufl. 2017, Art. 261 N 10). Bezüglich des Verfügungsanspruchs hat das Gericht eine sog. Hauptsachenprognose zu stellen, bezüglich des Verfügungsgrundes eine sog. Nachteilsprognose (BSK-SPRECHER, a.a.O., N 12 zu Art. 261 N 12). Verfügungsanspruch kann grundsätzlich jede subjektive Berechtigung des Zivilrechts sein, die auf eine positive oder negative Leistung, Gestaltung oder Feststellung gerichtet ist. Die gesuchstellende

Partei muss ihren Verfügungsanspruch, die Begründetheit ihres materiellen Hauptbegehrens, glaubhaft machen (BSK-SPRECHER, a.a.O., Art. 261 N 15). Weiter muss die vorsorgliche Massnahme zur Abwehr des Nachteils notwendig sein. Mit Notwendigkeit ist gemeint, dass die Massnahme in zeitlicher und sachlicher Hinsicht als geeignet erscheint. Dabei darf die Massnahme nicht weiter gehen als zur Wahrung der materiellen Ansprüche erforderlich. Überdies muss sie auch verhältnismässig sein (BSK-SPRECHER, a.a.O., N 112 zu Art. 261 N 112). Eine vorsorgliche Massnahme kann jede gerichtliche Anordnung sein, die geeignet ist, den drohenden Nachteil abzuwenden, insbesondere etwa ein Verbot oder eine Anordnung zur Beseitigung eines rechtswidrigen Zustands (Art. 262 lit. a und lit. b ZPO).

E. 6.3

Hauptsacheprognose (Verfügungsanspruch): Verletzung von Art. 6 DSGVO

E. 6.3.1

Das Bundesgesetz über den Datenschutz (DSG) gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch private Personen und Bundesorgane (Art. 2 Abs. 1 DSG). Dabei fallen unter den Begriff "Personendaten" alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, wobei natürliche oder juristische Personen von der Bearbeitung betroffen sein können (Art. 3 lit. a und b DSG). "Bearbeiten" ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaf-

- 12 - fen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (Art. 3 lit. e DSG). Unter "Bekanntgabe" wird gemäss Art. 3 lit. f. DSG das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben und Veröffentlichen verstanden. Gemäss Art. 6 Abs. 1 DSG gilt als schwerwiegende Gefährdung der Persönlichkeit von Gesetzes wegen (d.h. im Sinne einer unwiderlegbaren Vermutung) jede Bekanntgabe in ein Land, welches über keine angemessene Datenschutzgesetzgebung verfügt (ROSENTHAL, in: Rosenthal/Jöhri (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008, N 27 zu Art. 6 Abs. 1). Das hiesige Handelsgericht und anschliessend das Bundesgericht haben bereits (mehrfach) festgehalten, dass die USA nicht über eine Gesetzgebung verfügen, die einen angemessenen Datenschutz im Sinne von Art. 6 Abs. 1 DSG gewährleistet (Urteile des Bundesgerichts 4A_250/2018 vom 1. Oktober 2018 E. 4 und 4A_83/2016 vom 22. September 2016 E. 3.1; Urteile des Handelsgerichts des Kantons Zürich HG150022-O vom 24. November 2017 E. 2.3.2.; HG150018-O vom 1. September 2017 E. 2.3.4.3.; HG150254-O vom 21. Juni 2017 E. II.1.2.2.; HG150048-O vom 14. Juni 2016 E. 4.1. m.w.H.; HG140186-O vom 16. Dezember 2015 E. 5.3.1).

E. 6.3.2

Strittig sind vorliegend insbesondere zwei Fragen: Zum einen, ob dem Kläger 2 eine Aktivlegitimation zukommt und zum anderen, ob überhaupt eine Lieferung von Personendaten i.S.d. Art. 3 DSG an das DoJ droht.

E. 6.3.3

Zur Frage der Aktivlegitimation des Klägers 2 Die Beklagte bringt vor, der Kläger 2 sei weder Kontoinhaber der streitgegenständlichen Konten, noch beabsichtige die Beklagte, irgendwelche ihn betreffenden oder identifizierbar machenden Daten gegenüber dem DoJ

offenzulegen. Deshalb komme ihm mangels Anspruchsgrundlage keine Aktivlegitimation zu (act. 11 Rz 84). Wie die Kläger zu Recht ausführen, beziehen sich die Informationen in der Leaver-Liste und dem Factsheet durchaus (auch) auf den Kläger 2 (act. 1 Rz 63). Die Beklagte selbst führt aus, der US-Bezug der streitgegenständlichen Konten

- 13 - bestehe darin, dass der Kläger 2 als bis im Jahr 2010 wirtschaftlich Berechtigter der Konten ein Domizil in den USA gehabt und politische Spenden in den USA gemacht habe (act. 11 Rz 57 ff.). Diese und weitere Informationen befinden sich auch im Factsheet, welches die Beklagte an das DoJ übermitteln möchte (act. 11/2). Die an das DoJ zu übermittelnden Daten betreffen somit klarerweise den Kläger 2. Wie nachfolgend aufzuzeigen ist, ist zudem auch glaubhaft, dass es sich dabei um Personendaten handelt, welche unter den Schutzbereich von Art. 6 DSGVO fallen. Der Kläger 2 ist somit zur Klage aktivlegitimiert.

E. 6.3.4

Zur Frage der drohenden Lieferung von Personendaten

E. 6.3.4.1

Die Beklagte führt aus, die dem DoJ zu übermittelnden Transaktionsinformationen seien anonymisiert bzw. dem gleichkommend pseudonymisiert. Namentlich habe sie (i) sämtliche Überweisungsbeträge in US-Dollar umgerechnet, (ii) die Transaktionen addiert und nur das monatliche Total ausgewiesen und (iii) das ermittelte Total auf die nächsten CHF 10'000.– aufgerundet. Auch die weiteren Informationen in der Leaver-Liste und dem Factsheet liessen keine Identifikation von Personen zu. Zum einen würden die Namen der Kläger nicht genannt. Zudem handle es sich bei den streitgegenständlichen Konten zugewiesenen C.____-Nummern weder um Konto- noch um Kundennummern. Es seien reine Kontrollnummern, welche es ausschliesslich der Beklagten erlaube, die dahinterstehende Kundenbeziehung zu identifizieren. Entsprechend handle es sich bei der zu übermittelnden Liste und dem Factsheet um keine Personendaten i.S.v. Art. 3 lit. a DSGVO, weshalb das Datenschutzgesetz nicht anwendbar sei (act. 11 Rz 41, 68 ff. und 85 ff.). Die Kläger stellen sich auf den Standpunkt, die Beklagte würde eine Anonymisierung der Daten in der Leaver-Liste und dem Factsheet nicht glaubhaft machen. Die zu übermittelnden Daten könnten aufgrund von Big-Data-Analysen bestimmbar gemacht werden. Konkret könne das DoJ etwa die Informationen aus der Leaver-Liste mit SWIFT-Daten (Society for Worldwide Interbank Financial Telecommunication) abgleichen und so die Identität der Kläger ermitteln. Ein Bank-

- 14 - kunde könne über Banktransaktionen, die er getätigt habe, leicht identifiziert werden (act. 1 Rz 85). Die Beklagte entgegnet, das DoJ könne nicht ohne Weiteres auf SWIFT-Daten zurückgreifen. Doch selbst bei einem unbeschränkten Zugriff auf SWIFT-Daten wäre eine Identifizierung der Kläger gemäss der Beklagten wegen der Pseudonymisierung der Daten nicht möglich. Darüber hinaus scheide eine systematische Auswertung schon aufgrund der Datenmenge aus, welche das SWIFT-System übermittle (act. 11 Rz 78 f.).

E. 6.3.4.2

Gemäss dem Bundesgericht sind pseudonymisierte Daten unter Umständen anonymisierten Daten gleichgestellt und dürfen infolgedessen auch gegen den Willen des Betroffenen geliefert werden, da sie nicht mehr Personendaten im Sinne der

Datenschutzgesetzgebung darstellen (vgl. Urteil des Bundesgerichts, 4A_365/2017, vom 26. Februar 2018, E. 5.2.1 und E. 5.3.1). Eine Person ist bestimmbar, wenn sich ihre Identität aus dem Kontext der Daten oder durch die Kombination mit anderen Daten ergibt, solange dies ohne unverhältnismässigen Aufwand möglich ist. Unverhältnismässig ist der Aufwand, wenn nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird. Beim Aufwand sind auch die technischen Möglichkeiten mitzubersichtigen, so etwa im Internet verfügbare Suchwerkzeuge oder Technologien wie Big-Data-Analytics. Nicht mehr bestimmbar ist eine Person, wenn Personendaten anonymisiert worden sind. Anonymisierung bedeutet, dass der Personenbezug irreversibel aufgehoben wird, dass ohne unverhältnismässigen Aufwand keine Rückschlüsse auf Personen mehr möglich sind. Anders als bei der Pseudonymisierung darf kein Schlüssel (Zuordnungsregel) aufbewahrt werden, der die Re-Identifikation der betroffenen Person ermöglicht. Bei einer Pseudonymisierung soll der Personenbezug aufgehoben werden, aber bloss reversibel. Der Schlüssel zur Re-Identifizierung der Informationen bleibt erhalten. Deshalb bleiben pseudonymisierte Personendaten für alle, die Zugang zum Schlüssel haben, weiterhin Personendaten. Massgeblich ist also, wo sich dieser Schlüssel befindet bzw. wer konk-

- 15 - ret Zugang dazu hat. Dass pseudonyme Daten grundsätzlich nicht als Personendaten im Sinne des Datenschutzgesetzes zu qualifizieren sind, kann also nicht gesagt werden. Angesichts der heute bereits verfügbaren technischen Möglichkeiten der Re-Identifizierung – Stichwort: Big-Data-Analytics – verbleibt für die irreversible Anonymisierung von Personendaten nur wenig Raum. In den meisten Fällen werden sich vermeintlich irreversible Anonymisierungen angesichts der heute bereits verfügbaren technischen Re-Identifizierungsverfahren und des äusserst breiten Umfangs des Personendatenbegriffs als reversibel erweisen. Dies umso mehr, als im Big-Data-Bereich eine Menge von anonymisierten Daten analysiert wird, was bedeutet, dass je grösser die Datenmenge ist, desto höher wird die Wahrscheinlichkeit, dass Daten einer bestimmten Person zugeordnet werden können (SHK DSG-RUDIN, Bern 2015, Art. 3 N 10 ff., m.w.H.; BSK DSG-BLECHTA, 3. Aufl., Basel 2014, Art. 3 N 12 f., m.w.H.; ROSENTHAL, Handkommentar DSG, Zürich 2008, Art. 3 N 35 ff., m.w.H.; BAERISWYL in: Weber/Thouvenin [Hrsg.], ZIK: Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, S. 52, m.w.H.).

E. 6.3.4.3

Da die Beklagte vorbringt, nur sie selbst könne die Kläger anhand der zu übermittelnden Daten identifizieren (vgl. act. 11 Rz 71), ist vorliegend bloss von einer Pseudonymisierung und nicht einer Anonymisierung auszugehen. Die Leaver-Liste enthält umfangreiche Transaktionsdaten; sie listen die von den klägerischen Konten getätigten oder empfangenen Zahlungen monatlich zusammengefasst auf unter Angabe der jeweiligen Sender- und Empfängerbanken (act. 3/11/1). Dabei ist darauf hinzuweisen, dass das US-Programm bekanntermassen keine anderen Währungen als US-Dollar erwähnt und die Addition der Transaktionen sowie die Ausweisung des monatlichen Totals sogar verlangt (Ziff. II.D.2.vi; act. 3/19 S. 4). Anders als von der Beklagten ausgeführt, sind darin also keine Anonymisierungsmassnahmen zu erkennen. Weiter ergeben sich aus der Leaver-Liste und dem Factsheet zwar nicht die Namen der Kläger, indessen ihre rechtliche Stellung in Bezug auf die Konten und deren Status als U.S.-Person (BO = beneficial owner, PoA = power of attorney, act. 3/11/1 und 3/11/2). Zudem sind im Factsheet ausser der

C. _____-Nummer

- 16 - und der Umrechnung und Aufrundung der Kontobestände keine Anonymisierungsmassnahmen ersichtlich. Insbesondere wurden hinsichtlich des wirtschaftlich Berechtigten – sprich des Klägers 2 – Angaben über seine Nationalität ("dual belgian-israeli national"), seinen Wohnort ("residing in Switzerland"), seine Beziehung zum zweiten wirtschaftlich Berechtigten (BO1 son, BO2 father) sowie zu seinem Verhalten in den USA ("...may permanently live in the U.S ... made contributions to U.S. political campaigns ... may have U.S. addresses and phone numbers") gemacht. Im Zusammenhang mit den Transaktionsdaten der Leaver-List scheint damit eine Bestimmbarkeit der Kläger zumindest glaubhaft gemacht, weshalb von Personendaten i.S.d. Art. 3 DSGVO auszugehen ist. Zuletzt vermag die Beklagte die mit Beweismitteln unterlegten Ausführungen der Kläger nicht zu entkräften, wonach die US-Behörden Zugriff auf SWIFT-Daten hätten und durch einen Datenabgleich so die Kläger eindeutig identifizieren könnten (vgl. act. 1 Rz 53 ff.). Die blossе Bestreitung und der Verweis auf die Website der SWIFT genügen dabei nicht. Zumal aus besagter Beilage auch hervorgeht, dass sich zumindest eines der SWIFT-Rechenzentren in den USA befindet (act. 12/27). Angesichts der Entwicklungen in der jüngsten Zeitgeschichte (Überwachungs- und Spähaffäre, CIA-Leaks) sind die technologischen und administrativen Möglichkeiten der US-Behörden – gerade im Bereich der massenhaften Datenbeschaffung und -analyse – kaum zu unterschätzen, genauso wie ihr Wille, diese auch einzusetzen. Aus dem "gigantischen" Umfang der SWIFT-Daten (act. 11 Rz 78 ff.) kann die Beklagte somit nichts zu ihren Gunsten ableiten. Vor diesem Hintergrund läuft das beklagte Vorbringen ins Leere, wonach es dem DoJ nicht möglich sei, eine solche Datenmenge zu analysieren, und wenn doch, es nach der allgemeinen Lebenserfahrung nicht zu erwarten sei, dass das DoJ einen solchen Aufwand auf sich nehmen würde (act. 11 Rz 80).

E. 6.3.4.4

Nach dem Gesagten ist glaubhaft gemacht, dass es sich bei den an das DoJ zu übermittelnden Daten um Personendaten i.S.v. Art. 3 DSGVO handelt und dass den Klägern durch die beabsichtigte Bekanntgabe eine Persönlichkeitsverletzung nach Art. 6 Abs. 1 DSGVO droht, welche nur bei Vorliegen eines Rechtfertigungsgrundes gemäss Art. 6 Abs. 2 DSGVO nicht widerrechtlich wäre.

- 17 -

E. 6.3.5

Rechtfertigungsgründe gemäss Art. 6 Abs. 2 DSGVO Die Beklagte ist für das Vorliegen von Rechtfertigungsgründen beweispflichtig. Solche macht sie aber nicht geltend. So tut sie etwa nicht dar, warum die Datenherausgabe zur Wahrung überwiegender öffentlicher Interessen – im Sinne der Rechtsprechung des Bundesgerichts und des hiesigen Gerichts – in concreto unerlässlich sei (vgl. act. 8 Rz. 51; vgl. zum Ganzen Urteil des Bundesgerichts, 4A_83/2016, vom 22. September 2016, E. 3.3.4; Urteil des Handelsgerichts HG150022-O vom 24. November 2017, E. 2.4.2.2). Die den Klägern drohende Persönlichkeitsverletzung ist damit nicht gerechtfertigt.

E. 6.4

Nachteilsprognose (Verfügungsgrund) Bei Eingriffen in absolute Rechte, wie den hier zur Diskussion stehenden Persönlichkeitsrechten der Kläger, werden die dadurch bewirkten

Nachteile kaum mehr zu beheben sein (Urteil des Handelsgerichts HE170022-O vom 29. Juni 2017 E. 3.1). Ein späteres Aufwiegen durch Geld stellt nur eine Hilfslösung dar, auf welche sich die betroffene Partei nicht einlassen muss (vgl. ZÜRCHER, in: DIKE-Kommentar zur ZPO, 2. Aufl., Zürich/St. Gallen 2016, N 31 zu Art. 261 ZPO). Vor diesem Hintergrund drohen den Klägern durch die Datenlieferung in die USA schwere Nachteile, die nicht mehr rückgängig gemacht werden können.

E. 6.5

Dringlichkeit Angesichts des Umstandes, dass ein vollständiges Durchlaufen des Hauptsacheprozesses erheblich länger dauern dürfte, ist die Dringlichkeit des vorsorglichen Verbotes der Datenherausgabe zu bejahen.

E. 6.6

Verhältnismässigkeit Die Parteien äussern sich nicht zur Verhältnismässigkeit der von den Klägern beantragten Massnahme.

- 18 - Insbesondere macht die Beklagte nicht geltend, dass es im Falle eines vorsorglichen Verbots zu einer Anklageerhebung durch das DoJ käme. Damit eine solche Gefahr bejaht werden könnte, hätte sie konkrete diesbezügliche Hinweise aufzeigen müssen. Umgekehrt ist offensichtlich, dass nur Art. 292 StGB den Klägern einen genügenden Schutz bietet (vgl. Urteil des Handelsgerichts des Kantons Zürich HE170477-O vom 26. Februar 2018 E. 4b; Urteil des Obergerichts des Kantons Zürich LF150002-O vom 3. März 2015 E. 5.5). Das Verbot der Datenherausgabe erweist sich insgesamt als verhältnismässig. Ein mildereres Mittel ist nicht ersichtlich.

E. 6.7

Fazit Die Kläger vermochten glaubhaft darzutun, dass sie in ihren Persönlichkeitsrechten verletzt werden könnten. Rechtfertigungsgründe liegen keine vor und wurden auch nicht gehörig dargetan. Das Verbot einer Datenherausgabe an das DoJ erweist sich als verhältnismässig und ist vorsorglich zu bestätigen. Die Klage ist gutzuheissen. Hiervon ausgenommen ist, wie oben erwogen, mangels Rechtsschutzinteresse die Datenübermittlung an andere US-Behörden als das DoJ und allgemein ins Ausland. Aus Gründen der Verhältnismässigkeit rechtfertigt es sich jedoch, das diesbezügliche Superprovisorium nicht sofort aufzuheben.

E. 7

Kosten- und Entschädigungsfolgen Die Regelung der Kosten- und Entschädigungsfolgen ist gestützt auf Art. 104 Abs. 3 ZPO dem Hauptsachegericht vorzubehalten. Nur für den Fall, dass die Anordnung wegen Nichtanhängigmachens des Prozesses dahinfallen sollte, ist eine definitive (wenn auch bedingte) Anordnung zu treffen. Sowohl die Festsetzung der Gerichtsgebühr als auch die Festsetzung der Parteientschädigung richten sich in erster Linie nach dem Streitwert (§ 2 Abs. 1 lit. a GebV OG; § 2 Abs. 1 lit. a Anw-GebV). Auszugehen ist, wie in der Verfügung vom 15. März 2019 erwogen (act. 4), von einem Streitwert von CHF 1'000'000.–, was in Anwendung von § 4 Abs. 1 und 2 i.V.m. 8 GebV OG zu einer Gerichtsgebühr von CHF 15'500.– führt. Die Parteientschädigung ist in Anwendung von § 4 Abs. 1 und 2 i.V.m. § 9 Anw-

- 19 - GebV auf CHF 16'000.– festzusetzen. Mangels Darlegung der Berechtigung zum Vorsteuerabzug ist die (allfällige) Parteientschädigung der Beklagten praxisgemäss ohne Mehrwehrsteuerzuschlag zuzusprechen (vgl. Urteil BGer 4A_552/2015 vom 25. Mai 2016

E. 4.5). Der Einzelrichter verfügt:

Export aus OpenCaseLaw (CC0). Verbindlich ist allein der vom erlassenden Gericht veröffentlichte Originaltext. Quellen-URL siehe oben.