ments ausgelagert und von diesen durchgeführt werden (Auftragsverarbeitung), so sind in diesem Fall auch die damit einhergehenden Anforderungen zu prüfen und entsprechende Anpassungen der Verträge vorzunehmen.[53]

Die im Unternehmen angesiedelte Verarbeitung von personenbezogenen Daten sollte unabhängig von einer gesetzlichen Verpflichtung in ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO eingetragen werden, sodass ein Überblick über die jeweiligen Tätigkeiten besteht.[54] Dabei müssen die entsprechenden Anforderungen gem. Art. 30 Abs. 1 DS-GVO erfüllt werden. Die Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO erfordert eine umfassende Dokumentation aller damit im Zusammenhang stehenden Vorgänge, sodass gegenüber den Aufsichtsbehörden im Streitfall ein entsprechender Nachweis vorgelegt werden kann.[55] Darunter fällt auch der Nachweis, dass die Datenschutzgrundsätze eingehalten worden sind.

Es sollte daher bei jeglichen informationstechnischen Einrichtungen im Bereich des intelligenten Energiemanagements versucht werden, die unpräzisen Anforderungen aus Art. 5 Abs. 1 DS-GVO – so weit wie möglich – zu implementieren, um so eine gesicherte Position hinsichtlich des Nachweises gegenüber Aufsichtsbehörden einzunehmen.[56] Bei besonders risikobehafteter Verarbeitung durch neue Technologien kann auch eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO erforderlich sein. Auch hinsichtlich des Beschäftigtendatenschutzes ist ein solcher Fall denkbar und wäre zu prüfen. Zudem sollte durch das Unternehmen eine zeitnahe Erfassung aller aktuellen Entwicklungen und Veröffentlichungen im Datenschutzrecht erfolgen, sodass notwendige Anpassungsschritte frühzeitig eingeleitet werden können.

VI. Fazit

Die Entwicklungen im Bereich des Datenschutzes werden auch mit Inkrafttreten von DS-GVO und BDSG 2018 nicht abgeschlossen sein. Die technischen Entwicklungen – insbesondere im Zusammenhang mit Digitalisierung und intelligentem Energiemanagement – erfordern auch eine risikoadäquate Ausgestaltung der rechtlichen Vorschriften. Dabei sind sowohl der Beschäftigtendatenschutz als auch die Systemgestaltung betroffen. Eine Konkretisierung mittels bereichsspezifischer Regelungen ist sinnvoll und sollte aus Gründen der Rechtssicherheit angestrebt werden. Für Unternehmen ist es zurzeit von Bedeutung, die Anforderungen von DS-GVO und BDSG 2018 umzusetzen und die weiteren Entwicklungen im Bereich des Datenschutzes aufmerksam zu verfolgen. Bei Ausgestaltung der informationstechnischen Komponenten eines intelligenten Energiemanagements sollten bereits heute flexible Anpassungsmechanismen implementiert werden, die angesprochene datenschutzrechtliche Risiken – i.S.e. datenschutzfreundlichen Technikgestaltung – von vornherein ausschließen.

Steffen Braun, LL.M.,
ist Wissenschaftlicher Mitarbeiter in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel. Der Beitrag beruht auf einem Vortrag des Autors bei der DSRI-Herbstakademie 2017 in Heidelberg.

53 Zur Auftragsverarbeitung und den damit einhergehenden Anforderungen s. ausf. *Kort*, ZD 2016, 555, 557 f.; *Schmitz/von Dall'Armi*, ZD 2016, 427; *Lissner*, in: Taeger (Hrsg.), DSRITB 2016, S. 401 ff.
54 *Imping*, CR 6/2017, 378, 382.
55 *Imping*, CR 6/2017, 378, 382.
56 Werden entsprechende Dienstleistungen oder Anwendungssysteme extern „eingekauft", so ist die Erfüllung der datenschutzrechtlichen Anforderungen bei Dienstleister- bzw. Herstellerauswahl zu prüfen.

RECHTSPRECHUNG

Bezirksgericht Northern California: Deutsches Datenschutzrecht blockiert nicht die Vorlage von personenbezogenen Daten

Fed. R. Civ. P. 26(b)(1)
Entscheidung vom 8.11.2017 – Case No. 14-cv-01009-HSG (MEJ) – BrightEdge Technologies, Inc. v. Searchmetrics GmbH, et al.

Leitsätze der Redaktion

1. Eine Beklagte in einem in Kalifornien anhängigen Zivilverfahren in einer Patentsache kann sich nach Abwägung der Interessen nicht darauf berufen, dass eine Datensammlung personenbezogene Daten enthält, die nach deutschem Datenschutzrecht nicht in die USA übertragen werden dürfen.

2. Im Rahmen der erforderlichen Abwägung spricht insbesondere zu Gunsten der Vorlage im Wege des E-Discovery-Verfahrens, dass diese Daten durch eine Schutzverfügung des Gerichts (Protective Order) vor unberechtigten Zugriffen in den USA gesichert sind.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2017, 132018. Die Leitsätze wurden verfasst von RA *Dr. Axel Spies*, Morgan, Lewis & Bockius, Washington DC.

Aus den Gründen

1 Before the *Court* are two discovery letter briefs submitted by the parties. Having considered the parties' arguments and the relevant legal authority, the Court ORDERS production of the 2017 version of *Searchmetrics'* SugarCRM database, and all underlying documents referenced therein, for the following reasons.

E-Discovery
Datenzugriff
Datentransfer
Personenbezogene Daten

PROCEDURAL BACKGROUND

2 On October 17, 2017, Plaintiff *BrightEdge Technologies Inc.* (*BrightEdge*) and Defendants *Searchmetrics GmbH* and *Searchmetrics, Inc.* (collectively *Searchmetrics*) filed two Joint Discovery Dispute Letters with the *Court*. In the first letter, *BrightEdge* requested that the *Court* compel *Searchmetrics* to produce "all documents concerning sales, offers to sell, and attempted sales of Searchmetrics' products and the accused products", given the information's "relevance to infringement, willfulness, and damages." (Dkt. No. 169). In the second letter, *BrightEdge* asked that the *Court* compel production of *Searchmetrics'* SugarCRM database, as it is "relevant to willfulness, non-obviousness, and damages." (Dkt. No. 170). Searchmetrics asked that the *Court* deny both of *BrightEdge's* requests, stating that the information sought is not relevant (Dkt. Nos. 169, 170). *Searchmetrics* also argued that the first request is "overbroad, overly burdensome, (and) violates the relevancy and proportionality requirements of Fed. R. Civ. P. 26(b)(1)", and expressed con-

cerns that fulfilling the second request would result in a violation of German privacy laws. ...

3 On October 26, 2017, the *Court* held a hearing regarding this discovery dispute. October 26, 2017 Minute Entry, Dkt. No. 177.

4 On November 2, 2017, the *Superior Court of California for the County of Santa Clara* issued an order on a similar discovery dispute in the parties' trade secrets case. BrightEdge Technologies, Inc. v. Gabriel Martinez, et al., Case No. 2013-1-CV-256794 (*Santa Clara County Superior Court*). The *Superior Court* ordered *Searchmetrics* to produce the 2015 version of its SugarCRM database, given production would be made subject to the adequately protective Confidentiality Order already in place in that case.

LEGAL STANDARD

5 "Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case . . . . Information within this scope of discovery need not be admissible in evidence to be discoverable." Fed. R. Civ. P. 26(b)(1). "Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." Fed. R. Evid. 401. However, courts must limit discovery if the information sought "is unreasonably cumulative or duplicative, or can be obtained from some other source." Fed. R. Civ. P. 26(b)(2)(C)(i).

DISCUSSION

A. Second Letter Brief Regarding Production of the SugarCRM Database (Dkt. No. 170)

6 Discovery should be allowed unless the information sought has "no conceivable bearing on the case." First Fin. Sec., Inc. v. Jones, 2017 U.S. Dist. LEXIS 128194, at *4 (*N.D. Cal*. Aug. 11, 2017) (citation omitted). This *Court* has already recognized that the requested information (contained in *Searchmetrics'* SugarCRM database and the underlying documents referenced therein) is relevant to *BrightEdge's* claims of willful infringement and to the calculation of damages in this action (Dkt. No. 56 at 5). This *Court* has also recognized that this information cannot be obtained elsewhere. ... at 7. Additionally, at the October 26th hearing, *BrightEdge* stated that it is a common industry practice to produce this kind of database in this kind of litigation.

7 However, *Searchmetrics* has again asserted that transmitting the database and other related documents to a United States company would violate German privacy law (Dkt. No. 170 at 5; see also Dkt. No. 48). *Searchmetrics* alleges that the database and related documents contain personal data, which German law bars from being transferred "to countries lacking the same levels of protection afforded in EU countries [– countries such as] the United States." (Dkt. No. 170 at 5). Still, "the party opposing discovery has the burden of showing that discovery should not be allowed, and also has the burden of clarifying, explaining (,) and supporting its objections with competent evidence." La. Pac. Corp. v. Money Mkt. 1 Inst'l Inv. Dealer, 285 F.R.D. 481, 485 (N.D. Cal. 2012) (citations omitted); see DirectTV, Inc. v. Trone, 209 F.R.D. 455, 458 (C.D. Cal. 2002); see also Oakes v. Halvorsen Mar. Ltd., 179 F.R.D. 281, 283 (C.D. Cal. 1998) (citation omitted). *Searchmetrics* has failed to do so. *Searchmetrics* has twice made this general assertion, but has not explained why the protective order already in place in this case would not be sufficient to protect the private information contained in the database and related documents.

8 As this *Court* has already stated, even where a party seeks to prevent disclosure of documents based on foreign law, "it is well settled that such (foreign) statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute." Societe Nationale Industrielle Aerospatiale v. U.S. District Court, 482 U.S. 522, 544 n. 29 (1987) (citing Societe Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers, 357 U.S. 197, 204-06 (1958)). This *Court* previously ruled in favor of disclosure on a similar Joint Discovery Dispute Letter in this case. Dkt. No. 56. While related to a broader set of requests, the requests listed in that letter included one for *Searchmetrics'* SugarCRM database and the related documents (Dkt. No. 48 at 2).

9 In that letter, *Searchmetrics* similarly asserted objections to production based on German privacy law. However, in its order, this *Court* applied the relevant balancing test (set forth in Restatement (Third) of Foreign Relations Law section 442(1)(c) (1987) and stated in *Aerospatiale*, 482 U.S. at 544 n. 28 (1987)) and determined that the balance weighed in favor of compelling *Searchmetrics* to produce what it had previously withheld on the basis of international privacy law.

10 Nothing has changed. *Searchmetrics'* privacy concerns are addressed by the fact that production of the SugarCRM database and the underlying documents referenced therein will be subject to the protective order already in place. Therefore, the *Court* ORDERS production of the SugarCRM database and the underlying documents referenced therein.

B. First Letter Brief Regarding Requests for Production Nos. 21-22 (Dkt. No. 169)

11 At the October 26, 2017 hearing, *BrightEdge's* counsel informed the *Court* that the information requested in the first joint letter could be found in the SugarCRM database and the underlying documents referenced therein. October 26, 2017 Minute Entry; Transcript of Proceedings Held on October 26, 2017, Dkt. No. 180 at 20:11-14. The production requested in the first letter would therefore be duplicative, and its duplicate production is unnecessary.

12 Accordingly, the request is MOOT**.**

CONCLUSION

13 Therefore, the *Court* ORDERS production of the 2017 version of *Searchmetrics'* SugarCRM database and all underlying documents referenced therein. ...

Anmerkung

RA Dr. Axel Spies, Morgan, Lewis & Bockius, Washington DC

1. Wer die Entscheidungen der *US-Richter* zur internationalen E-Discovery verfolgt, sollte sich über diesen Beschluss der Einzelrichterin (Magistrate Judge) *James* vom eher weltoffenen *Bundesgericht für den Bezirk Northern California* nicht wundern. Im Kern streiten sich die Partien um die Optimierung von Suchmaschinen und fünf lukrative Patente – aber so viel nur am Rande. Viel interessanter ist der Zusammenhang mit dem deutschen Datenschutz. Bei der E-Discovery geht es im Zivilprozess darum, dass die Parteien für den Prozess die notwendigen Dokumente austauschen, also letztendlich um die Wahrheitsfindung (*Spies*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 2. Aufl., Teil XI, Kap. 2 Rdnr. 2).

Das meist teure E-Discovery-Verfahren kann Tausende, manchmal Millionen oder noch mehr von elektronisch gespeicherten Dokumenten umfassen (E-Mails, Berichte, Vermerke, Zeichnungen, Tabellen usw.). Der US-Richter eilt den Parteien nur zu Hilfe,

wenn sie miteinander bei der Dokumentenvorlage nicht zurechtkommen und Streifragen entschieden werden müssen (*Spies*, a.a.O., Rdnr. 3). Gerne tut er das nicht. Für manche Datenschutzexperten in Europa ist das massenweise, ungefilterte Absaugen von riesigen Datenmengen im Wege der E-Discovery in die USA eine datenschutzrechtliche Sünde, die einen fast auf den Scheiterhaufen bringen kann. In anderen Fällen „passiert" die Übermittlung einfach, „ohne viel Aufhebens zu machen". Wer die Durchführung einer E-Discovery in einem internationalen Unternehmen rechtlich begleitet, wird feststellen, dass sie zu handfesten Konflikten zwischen verschiedenen Stellen im Unternehmen führt.

2. In den USA droht einer Prozesspartei Ungemach, wenn sie nicht voll bei der E-Discovery kooperiert. Aber es gibt Grenzen. Dreh- und Angelpunkt für die US-Richter ist einmal mehr auch in Zeiten von Big Data eine dreißig Jahre alte Leitentscheidung des *US Supreme Court* i.S. Société Nationale Industrielle Aérospatiale (481 U.S. 522). Hiernach müssen die US-Richter bei einem der E-Discovery entgegenstehenden ausländischen Gesetz anhand von fünf Kriterien entscheiden, ob die Dokumentenvorlage doch noch zu erfolgen hat. Die Interessen des Staates, in welchem sich die Dokumente befinden, spielen bei der Abwägung eine Rolle, sind beileibe aber nicht der einzige Faktor (*Spies,* a.a.O., Rdnr. 9 f.). Ein aus seiner Sicht bestehendes Blocking Statute, das der Wahrheitsfindung in den USA entgegensteht, muss der US-Richter nicht beachten.

3. Die o.g. Discovery Order war vorauszusehen. Bundesrichterin *James* hatte bereits zu Beginn des Rechtstreits im August 2014 über E-Discovery-Fragen grds. entschieden. Der „Abwägungstest" nach der Aérospatiale-Rspr. führe auch jetzt zum Ergebnis, dass *Searchmetrics* die relevanten Aufzeichnungen im Verfahren vorzulegen hat, auch wenn die Gesellschaft damit womöglich gegen deutsches Recht verstoße. In dieser Entscheidung stellt die *Richterin* die Behauptung des deutschen Unternehmens in Frage, dass es auf Grund der Offenlegungen mit Strafmaßnahmen konfrontiert werden würde. Sie schreibt weiter, dass „Searchmetrics kein Argument vorgebracht hat, dass bei einer Übermittlung von persönlichen Daten Geldbußen unter ähnlichen Umständen verhängt würden." Die US-Tochtergesellschaft von *Searchmetrics* könne sich nicht hinter dem deutschen Datenschutzrecht verstecken.

Damit ging die *Richterin* weiter als z.B. die Richterkollegen aus Utah im Fall Access Data v. Alste (MMR 2010, 275 f. m Anm. *Spies/Schröder*). In diesem Verfahren hatte das *Gericht* den Status des BDSG als Blocking Statute offen gelassen und als salomonischen Ausgleich eine beschränkte Discovery für in Deutschland belegene Dokumente zugelassen. Gemeinsam ist beiden Entscheidungen, dass das Vorliegen einer Protective Order für die Daten aus der EU eine wichtige Rolle bei der o.g. Abwägung spielt. In einer solchen Schutzanordnung kann das US-Gericht z.B. anordnen, dass nur besonders beauftragte Anwälte oder geschulte Experten Zugang zu den Daten haben dürfen, ferner dass die Daten getrennt und an einem sicheren Ort gespeichert werden müssen, usw. (näher *Spies,* a.a.O., Rdnr. 42.) Eine in den USA gebräuchliche Vorlage für eine Protective Order für die internationale E-Discovery mit zahlreichen Details hat die *Sedona Conference* (*Working Party 6*) entwickelt (näher *Spies*, a.a.O., Rdnr. 27 f.). Das eigentlich für die internationale Übermittlung von Beweismitteln im Zivilprozess vorgesehene HaagBewÜK v. 18.3.1970, das die USA wie Deutschland ratifiziert hat, hat die *Richterin* erst gar nicht erwähnt; es fristet in der Praxis ein Aschenputtel-Dasein.

4. Der Nachweis, dass nach der Rspr. des *US Supreme Court* in Aérospatiale deutsches oder europäisches Datenschutzrecht der Vorlage von Dokumenten im Zivilverfahren entgegensteht, ist mühsam und aufwändig. In den bekannt gewordenen Fällen verlangen die Richter ein eidliches Expertengutachten oder zumindest eine schriftliche Stellungnahme der deutschen Datenschutzbehörde bezogen auf den konkreten Fall. Die Daten dürfen nicht schon in den USA sein (Stichwort: Mirror Server in den USA). Eine Prozesspartei, die ohne große Hindernisse auf die Daten von den USA aus zugreifen kann, hat vor dem US-Richter schlechte Karten. Im hier geschilderten Verfahren hatte die Tochtergesellschaft der Bekl. die SugarCRM-Datenbasis genutzt und versucht, auf diesem Wege einige wichtige Daten außerhalb der USA abzuladen, so zumindest der Klägervortrag.

Selbst wenn man in der Argumentation mit dem deutschen Datenschutz soweit in der Sache Gehör findet, muss die Partei den Richter auch noch davon überzeugen, dass es auch praktisch für die Partei zu erheblichen Nachteilen führt, wenn sie nach US-Recht die gewünschten Dokumente im Wege der E-Discovery vorlegt. „A tall order", wie man in den USA sagen würde.

5. Noch weiter geht eine neue Entscheidung des *US District Court for Southern District of Michigan* (Knight v. Henkel v. 30.11.2017 (WL 5898455)). Ein aus Deutschland von der Bekl. eingeflogener bekannter Rechtsexperte drang vor Gericht nicht durch, u.a. weil er nicht überzeugend darlegen konnte, dass der Bekl. bei einer Verletzung des BDSG Strafen drohen. Richter *Lawson* kritisierte in der Entscheidung den Experten massiv und war der Überzeugung, dass er selbst § 4c Abs. 1 Satz 4 BDSG aus US-Sicht nach dessen Wortlaut auslegen könne, wonach die Datenübermittlung aus Deutschland in die USA „zur Verteidigung von Rechtsansprüchen" erlaubt sei. Auf Grund dessen urteilte er angesichts der Bedeutung der in Deutschland gespeicherten Dokumente für den Prozess zu Gunsten der E-Discovery gegen die Bekl. (a.a.O., S. 12 f.). Richter *Lawson* berief sich auf die Grundentscheidung des US-Verfassungsrechts von 1803 (Marbury v. Madison), in der es heißt: „It is ... the duty of the judicial department to say what the law is."

6. Vielleicht ändert sich diese Rechtsprechung in den USA, wenn die Datenschutzbehörden in der EU für internationale Datentransfers einmal abschreckungswirksame Strafen nach der DS-GVO bei unerlaubter E-Discovery verhängen. Nach der gegenwärtigen Rechtslage scheint soweit noch keine Behörde und kein deutsches Gericht gegangen zu sein. Sehr verwunderlich ist die Zurückhaltung nicht, da bei einer Sanktionierung des Datenflusses in die USA durch ein hohes Bußgeld der Partei möglicherweise die Verteidigung im US-Prozess abgeschnitten würde, die nach Art. 49 Abs. 1 lit. e DS-GVO ein beschränktes Übermittlungsprivileg zur „Ausübung oder Verteidigung von Rechtsansprüchen" auch in ein unsicheres Drittland genießt (*Schröder,* in: Kühling/Buchner, Art. 49 DS-GVO Rdnr. 26). Und würde ein solches Bußgeld gegen ein Unternehmen wirklich in den USA helfen? Entweder die Partei hat die Daten schon übermittelt, dann ändert auch ein Bußgeld nichts, dass die Daten schon in den USA sind. Oder die Partei weist darauf hin, dass zumindest in einem ähnlich gelagerten Fall ein Bußgeld verhängt wurde: Dann müsste die betroffene Partei weiterhin dem US-Richter nachweisen, dass ihr auch eine solche Strafe droht. Wie man es dreht und wendet: Daran, dass die Partei diese erhebliche Hürde mit einem substanziierten Vortrag überwinden muss, wird auch die DS-GVO nichts ändern. Am besten ist, die Parteien einigen sich i.R.d. ohnehin von US-Prozessrecht vorgesehenen Meet & Confer (vgl. *Spies*, a.a.O., Rdnr. 39) und suchen möglichst gemeinsam mit den betroffenen datenschutzrechtlichen Stellen nach einem gangbaren Ausweg im Einzelfall.