

Compliance Berater

11 / 2020

Betriebs-Berater Compliance

28.10.2020 | 8.Jg
Seiten 405–448

EDITORIAL

Sind DSGVO-Schadensersatzansprüche ein Compliance-Risiko? | I

Tim Wybitul, RA

AUFSÄTZE

Compliance-Management für Zahlungsinstitute und E-Geld-Institute | 405

Anika Feger, RAin

Die wichtigsten kapitalmarktrechtlichen Publizitätspflichten im Überblick | 412

Dr. Thorsten Kuthe, RA, und Dr. Gero Lingen, RA

Kryptowerte: Hinweise und Besonderheiten betreffend die Prävention von Geldwäsche und Terrorismusfinanzierung | 418

Kilian Trautmann und Michael Kissler

Compliance als Element des internen Kontrollsystems im polnischen Bankensektor | 424

Dr. Bartosz Jagura und Paweł Ryszawa

Europäische Daten in den USA: Weder sicherer Hafen noch sicheres Schild | 429

Dr. Jan Dörrwächter, RA, und Johannes Brinkkötter, RA

Das Verbandssanktionengesetz im Spannungsfeld zwischen Vorstand und Aufsichtsrat – Teil 2 | 432

Dr. Christoph Klahold, RA

RECHTSPRECHUNG

EuGH: EU-US-Datenschutzschild bietet keinen angemessenen Schutz | 437

CB-EDITORIAL

Sind DSGVO-Schadensersatzansprüche ein Compliance-Risiko?

Bis 2018 wäre kaum jemand auf die Idee gekommen, sich über Schadensersatzansprüche wegen Datenschutzverstößen ernste Gedanken zu machen. Verletzungen des Datenschutzrechts berühren zunächst Persönlichkeitsrechte und nicht Vermögensrechte. Immaterielle Schäden sind im deutschen Recht nur dort zu erstatten, wo dies gesetzlich vorgesehen ist, § 253 BGB. Das hat Art. 82 DSGVO geändert. Wer wegen eines Verstoßes gegen die DSGVO einen materiellen oder immateriellen Schaden erlitten hat, kann danach Schadensersatz fordern.

In Großbritannien wurden bereits Massenklagen auf DSGVO-Schadensersatz eingereicht. Die geltend gemachten Forderungen sollen nach Presseberichten Milliardenbeträge erreichen. Auch in Deutschland werben Verbrauchernanwälte und spezialisierte Legal Tech-Anbieter bereits um von möglichen Datenschutzverstößen betroffene Kläger. Wenn die Presse über Datenpannen berichtet, schalten sie oft schnell Werbung und stellen Plattformen online, auf denen sich mögliche Kläger registrieren können. Ein typisches Geschäftsmodell arbeitet mit Provisionen. Der Anbieter stellt den Anwalt, führt das Verfahren und trägt die Prozesskosten. Hat die Klage auf Schadensersatz Erfolg, so erhält der Anbieter 25 Prozent des eingeklagten Betrags.

Von Datenschutzverstößen sind oft sehr viele Verbraucher betroffen und die Sachverhalte sind meistens sehr ähnlich. Das macht es leicht, massenhaft Ansprüche einzuklagen – gerade, wenn man Legal Tech-Anwendungen einsetzt. Zumal es Regelungen der DSGVO gibt, die man zur Begründung von Schadensersatzforderungen nutzen kann. Die Anwälte der Kläger argumentieren dann oft, dass bereits ein subjektives Gefühl der Betroffenheit – etwa wegen der Offenlegung personenbezogener Daten – einen zu ersetzenden Schaden darstelle. Zudem müssten beklagte Unternehmen beweisen, dass sie die Vorgaben des Datenschutzes eingehalten hätten. Das Unternehmen solle nur dann von der Haftung befreit werden, wenn es nachweist, dass es in keiner Weise für den Schaden verantwortlich sei. Zudem seien zu ersetzende Schäden hoch anzusetzen. Denn nach Erwägungsgrund 146 der

DSGVO sollten Kläger einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten.

Deutsche Gerichte stehen bei solchen Verfahren noch am Anfang einer längeren Entwicklung. Viele Gerichte stehen Forderungen auf immateriellen Schaden wegen (tatsächlichen oder behaupteten) Datenschutzverstößen eher zurückhaltend gegenüber. In der Regel fordern die Richter, dass Kläger einen konkret erlittenen immateriellen Schaden darlegen müssen, etwa in Form einer öffentlichen Bloßstellung oder anderer wahrnehmbarer Nachteile. Ein Schaden sei nur dann anzunehmen, wenn es zu einer spürbaren Beeinträchtigung gekommen sei, sogenannte Erheblichkeitsschwelle.

Ganz anders hat sich jetzt das Arbeitsgericht Düsseldorf positioniert (Az. 9 Ca 6557/18). Es sprach einem Kläger wegen eines nach Auffassung der Richter verspätet und intransparent beantworteten Auskunftsantrags nach Art. 15 DSGVO immerhin 5.000 EUR Schadensersatz zu. Die Entscheidung sorgte teilweise für Unverständnis. Denn

wenn selbst kleinere Verstöße zu solchen Forderungen führen, könnten Klageforderungen bei ernsteren Übertretungen immense Höhen erreichen. Machen Kläger dann massenhaft Forderungen geltend, kann dies sogar den Bestand eines Unternehmens gefährden. Ebenso erstaunlich wie

die Höhe des Schadensersatzes ist auch die Begründung der Entscheidung. Das Gericht lehnte die Notwendigkeit einer erheblichen Beeinträchtigung ab. Dies sei nur eine Frage der Schadenshöhe. Zudem müsse Schadensersatz nach Art. 82 DSGVO wegen des europarechtlichen Effektivitätsgrundsatzes abschreckend wirken. Daher sei für dessen Höhe auch die wirtschaftliche Leistungsfähigkeit des Unternehmens maßgeblich.

Das Urteil ist nicht rechtskräftig und bislang eher ein Ausreißer. Aber wenn in den weiteren Instanzen auch andere Gerichte auf diesen Kurs einschwenken, kommt auf Unternehmen eine Menge zu. Daher zeigt das Urteil deutlich, dass beim Datenschutz nicht nur DSGVO-Bußgelder ein erhebliches Compliance-Risiko darstellen, sondern auch drohende Schadensersatzansprüche.

Massenhafte Forderungen können den Bestand eines Unternehmens gefährden.

Autor



Tim Wybitul ist Rechtsanwalt und Partner im Frankfurter Büro von Latham & Watkins. Er berät Unternehmen umfassend zu Fragen des Datenschutzes und angrenzenden Rechtsgebieten. Wybitul zählt zu den führenden Datenschutzanwälten in Deutschland.