REPUBLIK ÖSTERREICH
OBERSTER GERICHTSHOF

Der Oberste Gerichtshof hat durch den Senatspräsidenten Dr. Vogel als Vorsitzenden und die Hofräte Dr. Jensik, Dr. Musger, Dr. Schwarzenbacher und Dr. Rassi als weitere Richter in der Rechtssache der klagenden Partei A***** AG, *****, vertreten durch PHH Prochaska Havranek Rechtsanwälte GmbH in Wien, gegen die beklagte Partei S***** AG, *****, vertreten durch Diwok Hermann Petsche Rechtsanwälte LLP & Co KG in Wien, wegen Unterlassung, Beseitigung und Feststellung (Streitwert im Sicherungsverfahren 470.000 EUR), über den außerordentlichen Revisionsrekurs der beklagten Partei gegen den Beschluss des Oberlandesgerichts Linz vom 8. Juli 2016, GZ 3 R 88/16f-23, mit welchem der Beschluss des Landesgerichts Salzburg vom 25. Mai 2016, GZ 1 Cg 32/16x-18, bestätigt wurde, den

B e s c h l u s s

gefasst:

Dem außerordentlichen Revisionsrekurs wird nicht Folge gegeben.

Die beklagte Partei hat die Kosten des Revisionsrekurses endgültig selbst zu tragen. Die klagende

Partei hat die Kosten der Revisionsrekursbeantwortung vorläufig selbst zu tragen.

B e g r ü n d u n g :

Die Parteien erzeugen und vertreiben Ticket- und Eintrittssysteme für Skigebiete, Stadien und ähnliche Einrichtungen. Sie richten sich mit ihrem Angebot an dieselben Kundenkreise. Die Klägerin betreibt zudem Server, auf denen interne Anwendungen für ihre Kunden installiert sind. Sie speichert dort die mit der Nutzung der Eintrittssysteme verbundenen Daten ihrer Kunden. Diese haben über das Internet Zugang zu den Daten, wobei sie sich mit Benutzername und Passwort in die Datenbank einloggen müssen. Insbesondere können sie die Daten in Form von Berichten (etwa über Name und Anschrift der Käufer von Tickets in einem bestimmten Zeitraum) abrufen.

Solche Berichte wurden am Server, auf dem die Anwendung für den Kunden installiert war, standardmäßig in einem Zwischenspeicher („Cache“) abgelegt. Bei einigen dieser Server war es aufgrund der Verwendung einer Standardeinstellung möglich, unter Umgehung des Login-Vorgangs (mit Benutzername und Passwort) auf den Zwischenspeicher zuzugreifen. Dieser Zugriff erforderte jedoch mehrere Informationen, die einem Außenstehenden nicht bekannt waren und nur von IT-Spezialisten durch gezieltes Auskundschaften und Zuhilfenahme von Spezialsoftware erlangt werden konnten.

Insgesamt verfügte die Klägerin im strittigen Zeitraum über zehn Server, auf denen Applikationen für rund 150 Kunden installiert waren. Manche Kunden der Klägerin verfügen auch über einen eigenen Server, auf dem die

Klägerin für sie eine derartige Applikation betrieb. Dies war insbesondere bei einem der wichtigsten Kunden, dem Pool Ski Arlberg, der Fall. Auch bei diesem Server konnte man aus demselben Grund separat auf den Zwischenspeicher zugreifen.

Für einen unautorisierten Zugriff auf die Berichte waren nicht öffentliche Informationen erforderlich, die durch gezieltes Erkunden und Abfragen und eine gezielte Suche nach Schwachstellen im Sicherheitssystem der betroffenen Server gewonnen werden konnten. Diese Informationen waren vertraulich und von der Klägerin nicht veröffentlicht worden.

Anfang 2015 begann ein Mitarbeiter der Beklagten, unter Umgehen des Kennwortschutzes auf die betroffenen Server zuzugreifen. Die Benutzernamen und Kennwörter waren ihm von den Kunden der Klägerin nicht zur Verfügung gestellt worden. Bei einer „Mitbewerberanalyse“ hatte er bei einem dieser Kunden eine Bildschirmanzeige fotografiert, der eine bestimmte Internetadresse (URL) entnommen werden konnte. Nach dem Vorbringen der Beklagten konnten aufgrund dieser URL mit „trial and error“ unter geringfügiger Modifikation der IP-Adresse und Verwendung bestimmter Programmbefehle auch andere Berichte abgefragt werden. Ob der Mitarbeiter die Bildschirmanzeige mit Zustimmung des Kunden fotografiert hatte, konnten die Vorinstanzen nicht feststellen.

Insgesamt griff der Mitarbeiter der Beklagten zumindest zwölfmal auf Daten verschiedener Kunden der Klägerin zu, wobei er jeweils Befehle eingab, die zur Erstellung von Berichten führten. Aufgrund mehrerer Änderungen in den Anwendungen der Klägerin war ein solcher Zugriff ab Februar 2016 nicht mehr möglich; Zugriffsversuche des Mitarbeiters führten zu leeren Seiten.

Die Beklagte verwertete die durch die Zugriffe erhaltenen Informationen gezielt dazu, Kunden der Klägerin, jedenfalls den Pool Ski Arlberg, abzuwerben und der Klägerin beim Anwerben von Neukunden fehlende Datensicherheit zu unterstellen. Beim Pool Ski Arlberg ging sie dabei wie folgt vor: Ein Mitarbeiter nahm Kontakt mit dem Geschäftsführer einer dem Pool angehörenden Bergbahngesellschaft auf und berichtete ihm, dass aufgrund eines angeblichen Datenlecks bei der Klägerin Kundendaten „frei im Internet“ zugänglich seien. In diesem Zusammenhang übermittelte er ihm einen der abgerufenen Berichte (Gebietsübersichtsbericht Arlberg). Der Geschäftsführer leitete diese Information an „Opinion Leader“ des Pool Ski Arlberg weiter. Dabei sprach er von einem sorglosen Umgang der Klägerin mit den Daten ihrer Kunden.

Zur Sicherung ihres gleichlautenden Unterlassungsbegehrens beantragt die Klägerin, soweit im Revisionsrekursverfahren relevant, der Beklagten mit einstweiliger Verfügung zu verbieten,

> die widerrechtlich aus der Verfügungsmacht der Klägerin erlangten Daten zu nutzen und/oder nutzen zu lassen und oder gegenüber Dritten zu offenbaren.

Die Beklagte habe unberechtigt auf Server der Klägerin und des Pool Ski Arlberg zugegriffen und dabei gezielt den Kennwortschutz umgangen. Dabei sei sie rechtswidrig in ein fremdes Computersystem eingedrungen und habe sich dabei „(Kunden)Daten“ verschafft. Die von ihr auf diese Weise erstellten Berichte habe sie dazu verwendet, den Pool Ski Arlberg von der Klägerin abzuwerben und unter Hinweis auf Sicherheitsmängel bei der Klägerin neue Kunden zu gewinnen. Die Beklagte habe gegen § 6 Abs 1 DSG verstoßen und Daten entgegen § 7 DSG verarbeitet. Das

Verhalten der Leute der Beklagten sei auch strafbar nach den §§ 118a Abs 1 und 123 StGB sowie nach § 51 Abs 1 DSG. Dies begründe einen Anspruch nach § 1 UWG (Wettbewerbsvorsprung durch Rechtsbruch), zudem habe die Beklagte Geschäftsgeheimnisse weitergegeben (§ 11 Abs 2 iVm § 13 UWG).

Die Beklagte wendet, soweit im Revisionsrekursverfahren relevant, Folgendes ein: Bei den Daten der Bergbahnen habe es sich nicht um Geschäftsgeheimnisse der Klägerin gehandelt, weil sie einfach (also ohne Passwortschutz) zugänglich gewesen seien. Zudem sei die Klägerin nicht aktiv legitimiert, weil es sich nicht um ihre eigenen, sondern um die Daten ihrer Kunden gehandelt habe. Der Zugriff sei zudem nicht widerrechtlich erfolgt, weil nicht feststehe, dass der Kunde, bei dem der Mitarbeiter der Klägerin die Bildschirmanzeige fotografiert habe (was die Zugriffe ermöglicht habe), mit dieser Vorgangsweise nicht einverstanden gewesen sei. Die Beweislast treffe insofern die Klägerin.

Das Erstgericht erließ die einstweilige Verfügung. Die Beklagte habe „sittenwidrig“ iSv § 1 UWG gehandelt, weil sie widerrechtlich erlangte Daten benutzt habe, um die Klägerin anzuschwärzen. Darin liege auch eine Verletzung von Betriebs- und Geschäftsgeheimnissen iSv § 11 Abs 2 UWG. Die rechtswidrigen Zugriffe auf die Server und die Verwendung und Weitergabe von Daten fielen zudem in die Fallgruppe „Wettbewerbsvorsprung durch Rechtsbruch“ und verstießen daher auch gegen § 1 UWG.

Das Rekursgericht bestätigte diese Entscheidung. Es sprach aus, dass der Wert des Entscheidungsgegenstands 30.000 EUR übersteige und der ordentliche Revisionsrekurs

mangels Vorliegens einer erheblichen Rechtsfrage nicht zulässig sei.

Bei den mit Benutzername und Passwort geschützten Daten habe es sich um Geheimnisse iSv § 11 Abs 2 UWG gehandelt. Da die Zustimmung des Kunden zum Abfotografieren der Bildschirmanzeige nicht bescheinigt sei, sei jedenfalls von einem unlauteren Erlangen der Informationen auszugehen. Die Daten hätten sich in der faktischen Verfügungsmacht der Klägerin befunden. Die Beklagte habe die Daten unbefugt zu Zwecken des Wettbewerbs verwertet.

Der gegen diese Entscheidung gerichtete außerordentliche Revisionsrekurs der Klägerin ist zulässig, weil die Rechtslage einer Klarstellung bedarf, er ist aber nicht berechtigt.

1. Nach § 11 Abs 2 UWG iVm § 13 UWG kann auf Unterlassung in Anspruch genommen werden, wer

> „Geschäfts- oder Betriebsgeheimnisse, deren Kenntnis er […] durch eine gegen das Gesetz oder die guten Sitten verstoßende eigene Handlung erlangt hat, zu Zwecken des Wettbewerbs unbefugt verwertet oder an andere mitteilt.“

Die Vorinstanzen haben den Tatbestand dieser Bestimmung als erfüllt angesehen. Die Beklagte wendet dagegen ein, dass (a) keine Geschäftsgeheimnisse vorlägen, weil die Daten leicht zugänglich gewesen seien, (b) es sich nicht um Geschäftsgeheimnisse der Klägerin gehandelt habe, weswegen sie nicht aktiv legitimiert sei, und (c) der Nachweis einer gegen das Gesetz oder die guten Sitten verstoßenden Handlung nicht erbracht sei, weil die Vorinstanzen zur behaupteten Zustimmung eines Kunden zum (die Datenabfrage nach dem Vorbringen der Beklagten ermöglichenden) Abfotografieren der Bildschirmansicht eine

Negativfeststellung getroffen hätten. Mit diesen Einwänden dringt das Rechtsmittel nicht durch.

2. Bei den strittigen Daten handelte es sich um Geschäftsgeheimnisse.

2.1. Betriebs- oder Geschäftsgeheimnisse sind Tatsachen und Erkenntnisse kommerzieller oder technischer Art, die bloß einer bestimmten und begrenzten Zahl von Personen bekannt sind, nicht über diesen Kreis hinausdringen sollen und an deren Geheimhaltung ein wirtschaftliches Interesse besteht (9 Os 7/70, SSt 41/32; RIS-Justiz RS0079599; zuletzt etwa 4 Ob 55/14p, *Betriebsgeheimnisse*). Der Geheimhaltungswille muss nicht ausdrücklich erklärt werden, sondern kann sich auch aus den Umständen ergeben; im Anwendungsbereich des § 11 Abs 1 UWG (Geheimnisverletzung durch Bedienstete) genügt es, dass sich ein durchschnittlicher Arbeitnehmer über diesen Willen des Unternehmers klar sein musste (4 Ob 394/86, *Tenniskartei*, ÖBl 1988, 13; RIS-Justiz RS0079599 [T1]; zuletzt etwa 4 Ob 55/14p, *Betriebsgeheimnisse*). Gleiches muss bei der Verletzung von Geschäftsgeheimnissen durch Dritte (§ 11 Abs 2 UWG) gelten. Auch hier genügt es daher, wenn sich aus dem Verhalten des Unternehmers ergibt, dass bestimmte – auch sonst nicht allgemein zugängliche – Informationen einem bestimmten Personenkreis vorbehalten sein sollen.

2.2. Diese Voraussetzung ist bei Daten erfüllt, die regulär nur durch das Einloggen in eine durch Passwort geschützte Datenbank eingesehen werden können. Denn diese Schutzvorkehrungen lassen erkennen, dass die Kenntnis dieser Daten einem bestimmten Personenkreis vorbehalten sein sollte. Der für die Anwendung von § 11 UWG maßgebende Geheimhaltungswille ist daher ohne weiteres erkennbar. Aus „Sicherheitslücken“, wie sie hier offenbar vorlagen, lässt

sich nichts Gegenteiliges ableiten. Denn mangelhafte Sicherheitsstandards erlauben bei aufrechtem Passwortschutz nicht den Schluss, dass der Unternehmer kein Interesse an der Geheimhaltung mehr hätte. Vielmehr müssen sowohl Beschäftigte (§ 13 Abs 1 UWG) als auch Dritte (§ 13 Abs 2 UWG) redlicherweise annehmen, dass dem Unternehmer diese Mängel nicht bewusst waren, sodass aus deren Vorliegen keinesfalls ein Wegfall des Geheimnischarakters abgeleitet werden kann.

2.3. Die am 5. Juli 2016 in Kraft getretene und bis 9. Juni 2018 umzusetzende RL (EU) 2016/943 *über den Schutz vertraulichen Knowhows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung* steht dieser Auffassung nicht entgegen. Die Beklagte stützt sich insofern auf Art 2 Abs 1 lit c dieser RL, wonach Informationen ua nur dann als „Geschäftsgeheimnis“ im Sinn der RL gelten, wenn sie

> „Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person [sind], die die rechtmäßige Kontrolle über die Informationen besitzt.“

Diese Argumentation scheitert aus zwei Gründen.

(a) Zum einen ist die Umsetzungsfrist noch nicht abgelaufen. Zwar darf das nationale Recht auch vor diesem Zeitpunkt (soweit möglich) nicht in einer Weise ausgelegt werden, die das Erreichen des mit der Richtlinie verfolgten Zieles ernsthaft gefährden würde (C-212/04, *Adeneler*, Rz 123). Damit wird allerdings auch nach Auffassung des EuGH kein Gebot richtlinienkonformer Auslegung schon vor Ablauf der Umsetzungsfrist begründet (C-212/04, *Adeneler*, Rz 115; ebenso *Nettesheim* in *Grabitz/Hilf/Nettesheim*, Das Recht der Europäischen Union, Art 288 Rz 133; *Vcelouch* in

Mayer/Stöger, EUV/AEUV, Art 288 AEUV Rz 62). Dass die bisherige Interpretation des Begriffs „Geschäftsgeheimnis“ das Erreichen der mit der Richtlinie verfolgten Ziele ernsthaft gefährdete, ist nicht erkennbar.

(b) Zum anderen können die Mitgliedstaaten auch nach Ende der Umsetzungsfrist nach Art 1 Abs 1 der RL einen weitergehenden Schutz von Geschäftsgeheimnissen vorsehen. Zwar gilt das nicht, wenn das weitergehende nationale Recht gegen bestimmte Vorschriften der Richtlinie verstieße. Es ist aber nicht erkennbar, dass dies bei der hier maßgebenden Interpretation des Begriffs „Geschäftsgeheimnis“ zuträfe. Insbesondere ist die zwingende Schutzausnahme nach Art 5 lit b der RL im konkreten Fall nicht anwendbar. Danach ist zwar das Offenlegen von Geschäftsgeheimnissen zur Aufdeckung eines „beruflichen Fehlverhaltens“ zulässig; dies allerdings nur dann, wenn es in der Absicht erfolgt, „das allgemeine öffentliche Interesse zu schützen“. Im Gegensatz dazu hat die Beklagte hier ausschließlich eigene Interessen verfolgt.

(c) Aus diesen Gründen ist nicht weiter zu prüfen, ob unbeabsichtigte Sicherheitslücken tatsächlich nach Art 2 Abs 1 lit c der RL das Vorliegen eines Geschäftsgeheimnisses *im Sinn dieser RL* ausschließen.

3. Bei den strittigen Daten handelt es sich (auch) um Geschäftsgeheimnisse der Klägerin.

Zwar stammen die Daten von ihren Kunden und beziehen sich auf deren geschäftliche Verhältnisse. Faktisch befanden sie sich jedoch in der Verfügungsmacht der Klägerin, und sie hatte auch ein erhebliches eigenes Interesse an deren Geheimhaltung, da sonst die Nichtverlängerung der Verträge oder Schadenersatzansprüche der Kunden (*Juranek*/*Stögerer*, Sicherheitslücken in der Unternehmens-

EDV und Haftungskonsequenzen, ecolex 2015, 955) drohten. Faktische Verfügungsmacht und eigenes Geheimhaltungsinteresse genügen bei wertender Betrachtung für die Annahme, dass die Daten auch in Bezug auf die Klägerin in den Schutzbereich des § 11 Abs 2 UWG fallen. Damit kann offen bleiben, ob die Klagebefugnis nach § 13 UWG tatsächlich auf den betroffenen Unternehmer beschränkt ist (*Thiele* in *Wiebe/Kodek*, UWG[2] § 13 Rz 51; *Duursma* in *Gumpoldsberger/Baumann*, UWG [2006] § 13 Rz 8; vgl auch 4 Ob 50/04p = SZ 2004/68 zum entsprechenden Problem im Datenschutzrecht), oder ob nicht das Interesse der Allgemeinheit am Unterbleiben von Angriffen auf fremde Computersysteme eine nach § 14 UWG zu beurteilende Klagebefugnis auch von Mitbewerbern rechtfertigt.

4. An der Rechtswidrigkeit des Erlangens der Daten (§ 11 Abs 2 UWG) durch Eindringen in das fremde Computersystem besteht kein Zweifel (6 Ob 126/12s, jusIT 2013/26 [*Staudegger*] = ZIR 2013, 224 [*Dörfler*]). Die Beklagte hat nach Erkennen der Sicherheitslücke gezielt auf verschiedene Server der Klägerin und eines von dieser betreuten Unternehmens (Pool Ski Arlberg) zugegriffen und von dort Daten, die faktisch in der Verfügungsmacht der Klägerin als EDV-Dienstleisterin waren, in verarbeiteter Form heruntergeladen. Die Beklagte stützt sich für die ihrer Ansicht nach dennoch fehlende Rechtswidrigkeit ausschließlich auf die Negativfeststellung zur Frage, ob ein Kunde einem Mitarbeiter der Beklagten das Abfotografieren der Bildschirmanzeige erlaubt habe oder nicht. Darauf kommt es aber nicht an. Denn selbst wenn der Kunde diese Erlaubnis erteilt hätte, folgte daraus nicht seine Zustimmung zu einer dadurch möglich werdenden Abfrage seiner Daten. Zudem hatte der Mitarbeiter der Beklagten die durch das

Abfotografieren erhaltenen Informationen auch zum Zugriff auf Daten von anderen Kunden der Klägerin genutzt. Dies konnte keinesfalls von der allfälligen Zustimmung durch den einen Kunden gedeckt sein.

5. Das Verwerten und Weitergeben der Daten bestreitet die Beklagte nicht. Damit besteht der Unterlassungsanspruch der Klägerin schon nach § 11 Abs 2 iVm § 13 UWG zurecht. Der Revisionsrekurs der Beklagten muss daher scheitern, ohne dass zu prüfen wäre, ob der Anspruch auch nach § 1 UWG begründet wäre (Wettbewerbsvorsprung durch Rechtsbruch wegen Verstoß gegen Datenschutz- oder Strafrecht; Verletzung der beruflichen Sorgfalt).

6. Die Kostenentscheidung gründet sich auf § 393 Abs 1 EO.

Oberster Gerichtshof,
Wien, am 25. Oktober 2016
Dr. V o g e l
Für die Richtigkeit der Ausfertigung
die Leiterin der Geschäftsabteilung: