RA Hon.-Prof. Dr. Clemens Thiele, LL.M. Tax (GGU)
Salzburg

jusIT 2014/98, 201

# Datenschutz- und Lauterkeitsrecht

Eine jüngst veröffentlichte Entscheidung[1] des 4. Senats hat die Möglichkeit, Verletzungen des Datenschutzrechts (DSG 2000) mit den Mitteln des Lauterkeitsrechts durchzusetzen – erstmals seit der UWG-Novelle 2007[2] – behandelt. Der vorliegende Beitrag erörtert das Verhältnis der durchaus als komplex zu beurteilenden Rechtsgebiete zueinander und versucht die erste Systematisierung einer datenschutzrechtlichen Unlauterkeit. Eine Zusammenfassung der Ergebnisse rundet das stark unionsrechtlich geprägte Bild ab.

**Deskriptoren:** Datenschutzrecht; Wettbewerbsrecht; Data-Breach-Notification; Offenlegungspflichten, datenschutzrechtliche; Informationspflichtenverletzung; Datenverarbeitung, Grundsätze; Datenverarbeitung, Zulässigkeit; Datenübermittlung, Zulässigkeit; Datenverarbeitungsregister; Meldepflicht; Vorabkontrolle; Datenschutzverletzung; Unterlassungsanspruch; Vorwerfbarkeit, subjektive; Vorsprung, nicht gerechtfertigter; Geschäftspraktiken, aggressive und irreführende

**Normen:** DSG 2000: §§ 1, 6 ff, §§ 13, 15, 17 ff, §§ 24 f, § 30 Abs 6, §§ 50a ff, §§ 51 ff; UWG: §§ 1, 1a, 2, 14, Z 10 Anh

## 1. Ausgangsfall[3]

### 1.1. Sachverhalt

Die spätere Klägerin war eine Reiseveranstalterin aus München und bot offline sowie online Pauschalreisen an. Der beklagte Marktbegleiter betrieb seit mehreren Jahrzehnten, zuletzt als eingetragener Unternehmer, ein Reisebüro mit Sitz in Oberösterreich. Für die Akquisition von Kunden warb er ua mit günstigen Pauschalreisen, so auch auf seiner Internetseite. Die Kunden des Beklagten konnten ihre Reisen in den Geschäftsräumlichkeiten buchen und im Internet formularmäßige Buchungsanfragen absenden. Eine Buchungsmöglichkeit im Internet bestand nicht; hierfür musste zuerst ein Anmeldeformular ausgefüllt und es mussten personenbezogene Daten bekannt gegeben werden. Der Beklagte hatte keine aktive Meldung bei der Datenschutzkommission über die Verwendung und Verarbeitung solcher nutzerseitig zur Verfügung gestellten Daten erstattet.

Im zugrunde liegenden Lauterkeitsprozess machte die Klägerin im Sicherungsverfahren neben Verstößen gegen Informationspflichten gem § 5 ECG und der Gewerbeordnung auch einen unlauteren Rechtsbruch nach § 1 Abs 1 Z 1 UWG geltend; dies wegen unterbliebener Meldung bei den Datenschutzbehörden. Der Beklagte wendete ein, dass die über ein Kontaktformular abgefragten und verarbeiteten Daten gem § 17 Abs 2 Z 6 DSG 2000 nicht meldepflichtig wären, weil es sich um eine Standardanwendung nach der Standard- und Musterverordnung 2004[4] handeln würde.

Die I. und II. Instanz wiesen den Sicherungsantrag ab. Der OGH hatte sich ua mit der Frage zu befassen, ob ein Verstoß gegen das Datenschutzgesetz 2000 eine Verletzung des UWG 2007 darstellen kann, sowie ob im konkreten Fall diesbezüglich eine Unlauterkeit vorzuwerfen wäre.

### 1.2. Die Entscheidung des Gerichts

Der OGH gab dem erhobenen Revisionsrekurs wegen der Verletzung der Informationspflichten iSd § 5 ECG Folge, wies aber im Übrigen insb den hier interessierenden Rechtsbruch wegen Verletzung des DSG 2000 ab, weil im konkreten Fall nicht ersichtlich wäre, dass die Gesetzesverletzung geeignet war, dem Beklagten einen sachlich nicht gerechtfertigten Vorsprung vor gesetzestreuen Mitbewerbern zu verschaffen. Mangels aktiver Meldung bei der Datenschutzkommission betreffend die Verwendung und Verarbeitung nutzerseitig zur Verfügung gestellter Daten lag zwar eine Gesetzesverletzung vor, jedoch wäre diese nicht spürbar (genug) gewesen.[5]

## 2. Meinungsstand in Österreich

### 2.1. Judikatur

Zwischen dem Inkrafttreten des Datenschutzgesetzes 2000 und der UWG-Novelle 2007 sind – soweit ersichtlich – lediglich drei höchstgerichtliche Entscheidungen zu vermerken, die sich am Schnittpunkt von Datenschutz- und Lauterkeitsrecht befinden.

1) OGH 24. 6. 2014, 4 Ob 59/14a (Dienst der Informationsgesellschaft) = in diesem Heft, jusIT 2014/109, 229 (*Thiele*) = MR 2014, 258 = wbl 2014/206, 599 = ZIR-Slg 2014/92 = ZIR 2014, 416 (*Thiele*).

2) BGBl I 79/2007, seither novelliert durch BGBl I 13/2013 und I 112/2013.

3) OGH 24. 6. 2014, 4 Ob 59/14a (Dienst der Informationsgesellschaft) = in diesem Heft, jusIT 2014/109, 229 (*Thiele*) = MR 2014, 258 = wbl 2014/206, 599 = ZIR-Slg 2014/92 = ZIR 2014, 416 (*Thiele*).

4) Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (StMV 2004), BGBl II 312/2004, mehrfach nov, zuletzt mit BGBl II 514/2013.

5) OGH 24. 6. 2014, 4 Ob 59/14a (Dienste der Informationsgesellschaft) = MR 2014, 258, 260 ISp Punkt 2.4.: *„Mangels aktiver Meldung bei der Datenschutzkommission betreffend die Verwendung und Verarbeitung nutzerseitig zur Verfügung gestellter Daten liegt auch eine Gesetzesverletzung vor. Dass diese allerdings auch geeignet wäre, der Beklagten einen sachlich nicht gerechtfertigten Vorsprung vor gesetzestreuen Mitbewerbern zu verschaffen (vgl RIS-Justiz RS0120712), ist nicht ersichtlich."*

*2.1.1. Unbefugte Datenweitergabe*[6]

In dem Anfang 2004 entschiedenen Fall gab ein Unternehmer ihm übertragene Mehrwertnummern entgegen einem gesetzlichen Verbot weiter. Die Beklagte betrieb eine Telekommunikationsanlage, mit der sie Telekommunikationsdienste verwaltete und TK-Daten übertrug. Im Rahmen dieser Geschäftstätigkeit hatte sie einzelne Mehrwertnummern, die sie selbst von anderen Diensteanbietern übertragen erhalten hatte, an zwei in England ansässige Unternehmen (Ltds) weitergegeben. Für die Zurverfügungstellung ihrer technischen Plattform und die Vermietung dieser Einzelnummern erhielt die Beklagte ein umsatzabhängiges Entgelt. Die englischen Ltds führten entgegen § 101 TKG 1997 Werbeanrufe an österreichische Kunden durch, bei denen eine Tonbandstimme die angerufenen Verbraucher in ein umständliches Gespräch über eine (unzutreffende) Gewinnermittlung verwickelte, um Umsatz zu generieren, da den Angerufenen € 1,81 pro Minute an Telefonkosten entstanden. Die Bundesarbeiterkammer klagte auf Unterlassung dieser Geschäftspraxis und stützte sich gegenüber der Beklagten auf einen Verstoß gegen § 101 TKG 1997 iVm § 1 UWG und gegen § 2 UWG jeweils iVm § 18 UWG.

Der OGH gab dem Sicherungsbegehren statt. Das gesetzliche Verbot in § 7 NVO iVm Abschnitt C Z 7.4 zweiter Absatz der Anlage 2 zur damals in Kraft stehenden Nummerierungsverordnung (NVO)[7] hatte nämlich den Zweck, Klarheit über den Betreiber der Nummern zu sichern, um diesen auch wirksam zur Verantwortung ziehen zu können. Der OGH verurteilte den Unternehmer für die unzulässigen Handlungen der Erwerber der Mehrwertnummern nach § 18 UWG als einen für Handlungen im Betrieb eines Unternehmens Verantwortlichen. Für das Verhältnis zwischen Datenschutz und Lauterkeitsrecht lässt sich aus der Entscheidung gewinnen: Wer eine Mehrwertnummer, die ihm zugeteilt ist, unzulässigerweise weitergibt, hat für UWG-widrige Handlungen im Zusammenhang mit der Nutzung dieser Nummer einzustehen. Bei derartigen Mehrwertnummern handelt es sich sowohl um personenbezogene Daten (ähnlich IP-Adressen) iSd DSG 2000 als auch um geschützte Zugangs- bzw Verbindungsdaten iS des TKG 2003. Bemerkenswert ist ferner, dass sich das lauterkeitsrechtliche Einstehen nicht nur auf Handlungen erstreckt, die unmittelbar unter der Nummer begangen werden, sondern auch auf die Werbung und Ankündigungen für diese Nummer.[8]

*2.1.2. Bruch des Datengeheimnisses*[9]

Im Anlassfall betrieb die Erstklägerin ua einen Gummiwarengroßhandel; die Zweitklägerin betrieb diesen vor ihr und brachte ihn in die Erstklägerin ein. Der spätere Erstbeklagte war bei der Zweitklägerin bis zu seiner Entlassung Anfang des Jahres 2003 im Ein- und Verkauf tätig und hatte dort umfassende Kenntnisse über Kunden und Lieferanten sowie über die Kalkulationsgrundlagen des Unternehmens erworben. Die zweitbeklagte Gesellschaft wurde 2002 in Tschechien gegründet und war ua in derselben Branche wie die Klägerinnen tätig. Sie verfügt in Österreich über keine Gewerbeberechtigung. Der Erstbeklagte war seit seiner Entlassung bei der Zweitbeklagten geringfügig beschäftigt.

Nachdem die Entlassung des Erstbeklagten ausgesprochen worden war, waren bei seiner früheren Arbeitgeberin (der Zweitklägerin) mehrere Angebote und Anfragen nicht mehr auffindbar, die der Erstbeklagte zu betreuen gehabt hatte. In der Folge versuchte der Erstbeklagte, von anderen Lieferanten der Klägerinnen Waren zu beziehen und weitere Kunden abzuwerben, in einem Fall einen Kunden, dem er einen Preis von 10 bis 13 % unter dem der Klägerinnen anbot und dessen letzte Bestellung bei der Zweitklägerin er im Jahr 2002 selbst bearbeitet hatte.

Für den 4. Senat war zunächst offenkundig, dass durch die Verwendung fremder Kunden- und Lieferantendaten für die Anbahnung eigener Geschäfte ein sachlich nicht gerechtfertigter Vorsprung erzielt werden kann. Es war daher weiter zu prüfen, ob der ehemalige Mitarbeiter mit der Verwertung seiner in seinem Dienstverhältnis erworbenen Kenntnisse datenschutzrechtliche Bestimmungen verletzt hatte. Im Ergebnis wurde eine Sittenwidrigkeit iSd § 1 UWG deshalb verneint, weil es sich bei Kunden- und Lieferantendaten sowie Verkaufskonditionen um „eigene" Daten des Unternehmens handeln würde. Die Verarbeitung eigener Daten fällt aber nicht unter das Datenschutzgesetz, weshalb auch keine Verletzung datenschutzrechtlicher Bestimmungen vorliegen kann.[10]

In der datenschutzrechtlichen Lehre[11] ist dieses – paradoxe – Judikat einhellig auf Ablehnung gestoßen. Der OGH hatte schlicht die Rollenverteilung im Datenschutzrecht missverstanden und im Ergebnis den Schutz von Wirtschaftsdaten ebenso wie das Datengeheimnis nach dem DSG 2000 ad absurdum geführt.[12] Der methodische Mangel der Entscheidung liegt darin, den entscheidenden Rollenwechsel nicht erkannt zu haben: Im ursprünglichen Verhältnis zwischen den Klägerinnen und ihren Kunden-/Lieferanten sind die Klägerinnen für die personenbezogenen Kunden-/Lieferantendaten (Kunden-/Lieferantenlisten) Auftraggeber iSd § 4 Z 4 DSG 2000, dh verantwortliche Datenverarbeiter. Die Kunden bzw Lieferanten sind insoweit Betroffene iSd § 4 Z 3 DSG 2000 und durch das Datengeheimnis nach § 15 iVm § 1 Abs 1 DSG geschützt. Das Datengeheimnis müssen ausdrücklich auch Mitarbeiter der Klägerinnen nach § 15 Abs 1 DSG 2000 (unter Strafe nach §§ 51, 52 DSG 2000) wahren. Dabei bleibt es aber nicht: Mit der Verwendung der Unternehmensdaten, die nun durch den ehemaligen Mitarbeiter erfolgt, kommt es zu einem Rollenwechsel. Nimmt der ehemalige Mitarbeiter die Kunden-/Lieferantenlisten mit, trifft ab sofort er die Entscheidung iSd § 4 Z 4 DSG 2000, diese personenbezogenen Daten für neue, nämlich seine Zwecke zu verarbeiten. Damit wird der ehemalige Mitarbeiter für diese Wirtschaftsdaten zum Auftraggeber und die Klägerinnen werden zu Betroffenen der Datenverarbeitungen bei der Zweitbeklagten – ein glatter Bruch des Datengeheimnisses aus Wettbewerbsabsicht.[13]

Hervorzuheben ist, dass die der Entscheidung zugrunde liegende Konstellation – ein gekündigter Dienstnehmer kopiert die Kundenlisten seines bisherigen Arbeitgebers, um diese beim neuen Dienstgeber zum Zweck der Kundenabwerbung zu verwenden – als typischer

6) OGH 20. 1. 2004, 4 Ob 217/03w (Telefonmehrwertdienste) = MR 2004, 136 = RdW 2004/373, 413 = SZ 2004/7.

7) BGBl II 416/1997; nunmehr Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 (KEM-V 2009), BGBl II 212/2009 idgF, mehrfach novelliert.

8) Zutreffend *Wessely*, Entscheidungsanmerkung, MR 2004, 138.

9) OGH 4. 5. 2004, 4 Ob 50/04p (Datengeheimnis) = ecolex 2004/415, 873 (krit *Knyrim*) = EvBl 2005/2, 23 = RdW 2004/540, 596 = SZ 2004/68.

10) OGH 4. 5. 2004, 4 Ob 50/04p (Datengeheimnis) = ecolex 2004/415, 873 (krit *Knyrim*) = EvBl 2005/2, 23 = RdW 2004/540, 596 = SZ 2004/68.

11) *Jahnel*, OGH: Kein Schutz von Unternehmensdaten nach dem DSG?, RdW 2005, 200; *Knyrim*, Kann man sich zum Schutz seiner Kundendaten nicht mehr auf das DSG 2000 berufen?, ecolex 2005, 873; *ders*, Datenschutzrecht² (2012) 298 f.

12) Ganz deutlich *Jahnel*, RdW 2005, 200 (201) mwN.

13) *Jahnel*, RdW 2005, 200 (201); *ders*, Handbuch Datenschutzrecht (2010) Rz 3/70; ebenso *Knyrim*, ecolex 2005, 873 (874).

Beispielsfall des strafbaren Datenmissbrauchs nach § 51 DSG 2000 gilt.[14]

*2.1.3. Unbefugte Datenermittlung*[15]

Im dritten Fall verbot der OGH einem Privatdetektiv, die Infrastruktur eines Mobilfunkbetreibers in Eigenregie zur Ortung von Personen zu nutzen, indem er die sog Cell-ID mittels Spezialsoftware auslas und mit Daten der geografischen Positionen der jeweiligen Mobilfunkmasten durch GPS-Ortung ermittelte. Das Ziel des beklagten Unternehmers war es, Ortungsdienstleistungen, sog Location Based Services, gegen Entgelt anzubieten. Der klagende Mobilfunkbetreiber, die T-Mobile, behauptete das schmarotzerische Ausbeuten fremder Leistung, nämlich des von T-Mobile betriebenen Mobilfunknetzes samt der Daten der Cell-ID. Bemerkenswerterweise hielt der OGH fest, dass die Spürbarkeit der beanstandeten Handlung für das Vorliegen einer entsprechenden Nachfrageverlagerung nicht danach zu beurteilen ist, welchen geschäftlichen Erfolg der Beklagte bisher mit seinem lauterkeitswidrigen Handeln erzielt hat, sondern danach, ob sein Verhalten potenziell geeignet ist, zu einer nicht bloß unerheblichen Nachfrageverlagerung zu führen. Dass sich der Beklagte sein eigenes Ortungssystem nur unter Benützung ganz wesentlicher Bestandteile eines fremden Systems verschafft hatte, in das er mit unlauteren Mitteln eingedrungen war, begründete die glatte Übernahme einer fremden Leistung nach § 1 UWG.

Bemerkenswert erscheint, dass der OGH völlig zu Recht interne Netzdaten der Mobilfunker als durch § 1 UWG geschützte Güter ansieht, handelt es sich doch um gesetzmäßig ermittelte (indirekt) personenbezogene Daten iSd DSG 2000, denen ein geschäftlicher Wert zukommt, wie aus der Vorgangsweise des Detektivs offensichtlich wird.

## 2.2. Literatur

Aus der Zeit vor der UWG-Novelle 2007 fällt – neben der bereits zitierten Literatur zu den dargestellten Judikaten – eine grundsätzliche Stellungnahme der Lehre[16] auf. Die beiden Autoren gelangen zur Auffassung, dass Datenschutzverstöße objektiv geeignet sind, dem Verletzer einen unlauteren Rechtsvorsprung vor gesetzestreuen Mitbewerbern zu verschaffen. Ob sie auch subjektiv vorwerfbar sind, bleibt einer Einzelfallbeurteilung nach § 1 UWG aF überlassen.

Im Zusammenhang mit der Direktwerbung in sozialen Netzwerken beschäftigt sich ein anderer Teil der Lehre[17] mit den lauterkeitsrechtlichen Konsequenzen eines Verstoßes gegen die Einwilligung zum Erhalt von Werbenachrichten nach § 4 Z 14 DSG 2000 iVm § 107 Abs 2 TKG 2003. Sie gelangen zum Ergebnis, dass bei Verletzung datenschutzrechtlicher Verpflichtungen ein unlauterer Rechtsbruch iSd § 1 UWG im Einzelfall durchaus argumentierbar ist.

In der österreichischen Kommentarliteratur[18] fehlt bislang – soweit ersichtlich – eine grundlegende Auseinandersetzung zum Verhältnis zwischen Datenschutz und Lauterkeitsrecht. Lediglich im Großkommentar zur Fallgruppe Ausbeutung[19] findet sich ein Hinweis, dass der Verstoß gegen Datenschutzbestimmungen nach Beendigung des Arbeitsverhältnisses ein die Unlauterkeit begründender besonderer Umstand sein kann, den der Ex-Arbeitgeber nach §§ 1, 14 UWG geltend machen kann.

## 3. Meinungsstand in Deutschland

Rechtsvergleichend lohnt diesmal ein Blick zum großen Nachbarn letztlich nur bedingt. Zum einen kennt die deutsche Datenschutzrechtslage ein den Meldungen iSd §§ 17 ff DSG 2000 vergleichbares System nicht. Zum anderen ist das Verständnis der Fallgruppe Rechtsbruch nach § 4 Nr 11 dUWG ein gänzlich anderes als in Österreich.

§ 4 Nr 11 dUWG geht davon aus, dass eine unlautere geschäftliche Handlung vorliegt, wenn ein Teilnehmer am Wettbewerb einer gesetzlichen Vorschrift zuwiderhandelt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln. Als Marktverhalten ist jede Tätigkeit auf dem Markt zu sehen, durch die ein Unternehmer auf die Mitbewerber, Verbraucher und sonstigen Marktteilnehmer einwirkt. Nach jüngerer Rsp[20] stellt die deutsche UWG-Praxis darauf ab, dass die marktverhaltensregelnde Norm, die gebrochen wird, auf europäischen Grundlagen beruhen muss. Dies erfüllen datenschutzrechtliche Bestimmungen jedenfalls, da sie auf EU-Richtlinien[21] zurückgehen. Die Instanzgerichte[22] sind noch uneinheitlich; der BGH hat sich bislang nicht abschließend geäußert.[23]

Aus der deutschen Diskussion lässt sich allerdings mit Blick auf das unionsrechtlich gleich ausgestaltete Datenschutzrecht der Richtlinien gewinnen, dass nach ErwGr 7 zur DS-RL das Datenschutzrecht dazu dienen soll, einen verfälschten Wettbewerb zu verhindern, maW einheitliche Wettbewerbsbedingungen im Binnenmarkt herzustellen. So bestimmt ErwGr 8 der eDS-RL den Abbau von Behinderungen des Binnenmarktes in der elektronischen Kommunikation. Datenschutzrechtliche Bestimmungen dienen daher grundsätzlich dem Leistungswettbewerb, sodass ihre Verletzung keiner besonderen Begründung für die Spürbarkeit, maW der geschäftlichen Relevanz, bedürfen sollte. Die geschäftliche Relevanz ist lediglich zB

14) *Unger*, Grundzüge des Datenschutzrechts (2012) 98; *Knyrim*, Datenschutzrecht², 294; vgl auch LG Linz 7. 12. 1999, 27 EVr 591/99, 27 EHv 123/99 = ARD 5120/27/2000.

15) OGH 15. 9. 2005, 4 Ob 113/05d (Friend Finder) = ecolex 2006/217, 499 *(Braunböck)* = lex:itec 2006 H 2, 18 *(Feichtinger-Burgstaller)* = MR 2005, 490 = ÖBl 2006/26, 119 (*Gamerith*) = RdW 2006/67b, 65; dazu *Knyrim/Podoschek*, Mobilfunk-Netzdaten sind schützenswert. Nutzung von Cell-IDs für fremde Anwendungen sittenwidrig, lex:itec 2006 H 4, 36; dies, Interne Daten eines Mobilfunksystems laut OGH nicht für jedermann frei nutzbar, JurPC Web-Dok 2006/2.

16) *Jahnel/Thiele*, Datenschutz durch Wettbewerbsrecht, ÖJZ 2004, 870 passim.

17) *Kusznier/Liebel*, Direktwerbung in sozialen Netzwerken, ecolex 2011, 831 (834).

18) *Kraft/Steinmair*, UWG Praxiskommentar (2014); *Gumpoldsberger/Baumann/Duursmar/Duursma-Kepplinger*, UWG Kommentar (2006) mit Ergänzungsband (2009).

19) *Wiebe* in Wiebe/Kodek, UWG² § 1 Rz 645 und FN 1584.

20) BGH 31. 3. 2010, I ZR 34/08 (Gewährleistungsausschluss) = CR 2010, 806.

21) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie – DS-RL), ABl L 281 vom 23. 11. 1995, 31 ff; Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – eDS-RL), ABl L 201 vom 31. 7. 2002, 37 ff, geändert durch RL 2006/24/EG des Europäischen Parlaments und des Rates vom 15. 3. 2006, ABl L 105 vom 13. 4. 2006, 54, und RL 2009/136/EG des Europäischen Parlaments und des Rates vom 25. 11. 2009, ABl L 337 vom 18. 12. 2009, 11.

22) *Für* eine Anwendung des UWG: OLG Stuttgart 22. 2. 2007, 2 U 132/06 = ITRB 2007, 252 (*Stadler*) = MMR 2007, 437; OLG Köln 14. 8. 2009, 6 U 70/09 = NJW 2010, 90; 19. 11. 2010, 6 U 73/10 (nrk) = CR 2011, 680 (*Eckhardt*) = IPRB 2010, 32 (*Mulch*) = JurPC Web-Dok 91/2011; OLG Karlsruhe 9. 5. 2012, 6 U 38/11 = NJW 2012, 3312 (*Schneider*) = WRP 2012, 1439; OLG Hamburg 27. 6. 2013, 3 U 26/12 = CR 2013, 596 = ITRB 2013, 226 (*Engels*) = K&R 2013, 601; KG Berlin 24. 1. 2014, 5 U 42/12 (Freundefinder-Funktion) = K&R 2014, 280; LG Frankfurt 18. 2. 2014, 3-10 O 86/12 (Webtracking) = CR 2014, 266 (krit *Laue/Nink*) = ITRB 2014, 204 (*Elteste*); *ablehnend* hingegen OLG Frankfurt 30. 6. 2005, 6 U 168/04 = WRP 2005, 1029; KG Berlin 29. 4. 2011, 5 W 88/11 (Sterntaufe) = K&R 2011, 418; OLG München 12. 1. 2012, 29 U 3926/11 = CR 2012, 269 = K&R 2012, 299.

23) Ansatzweise bereits BGH 22. 1. 2014, I ZR 218/12 (Nordjob-Messe) = GRUR 2014, 682; dzt anhängige Rs I ZR 224/10 (Rückgewinnung von Stromkunden) zu OLG Köln 6 U 73/10.

bei unwesentlichen Defiziten einer Datenschutzerklärung zu verneinen.

Gleichfalls zeichnet sich in der jüngsten deutschen Literatur[24] die Tendenz ab, dass Datenschutzrechtsverstöße zugleich als Lauterkeitsverstoß iSd § 4 Nr 11 dUWG bewertet werden: Es dürfte sich wohl jene Auffassung als herrschend durchsetzen, die eine Unlauterkeit bei Verstoß gegen Bestimmungen annimmt, die die Datennutzung für eigene oder fremde kommerzielle Zwecke regeln, insb die Missachtung der §§ 28, 29 BDSG. In Betracht kommen daher Verstöße gegen Bestimmungen, die zB die Voraussetzungen der Datennutzung für Werbezwecke oder den Adresshandel regeln, aber auch die telemedienrechtlichen Datenschutzbestimmungen, einschließlich sämtlicher Informationspflichten, die im Vorfeld einer Datenerhebung zu kommerziellen Zwecken, auch für den Abschluss eines Fernabsatzvertrages, zu erfüllen sind, also insb §§ 4, 4a BDSG, § 13 TMG, sowie die Verpflichtung gem § 28 Abs 4 Satz 2 BDSG und § 15 Abs 3 TMG, auf bestehende Widerspruchsrechte hinzuweisen.

## 4. Eigene Stellungnahme zur datenschutzrechtlichen Unlauterkeit

### 4.1. Einfluss der Richtlinie gegen unlautere Geschäftspraktiken

Die UGP-RL[25] enthält keine dem österreichischen Verständnis des Rechtsbruchtatbestandes entsprechende Regelung. Sie bezweckt in dem von ihr geregelten Bereich eine Vollharmonisierung nach Art 4 UGP-RL.[26] Die Vollharmonisierung besteht aber nur im Anwendungsbereich der UGP-RL, also im Verhältnis zu Verbrauchern (B2C).[27] Da der österreichische Gesetzgeber das UWG idF 2007 gleichermaßen auf den B2C- und den B2B-Bereich angewendet wissen will,[28] kommt es zu einer gespalteten Auslegung des Lauterkeitsrechts. Erfüllt daher ein unternehmerisches Verhalten für sich genommen nicht die Anforderungen an eine Geschäftspraktik iSv Art 2 lit d UGP-RL,[29] besteht – außerhalb des Anwendungsbereichs der Richtlinie – die Möglichkeit, nationales Lauterkeitsrecht vollumfänglich anzuwenden. So bleibt insb der Rechtsbruchtatbestand im B2B-Bereich uneingeschränkt anwendbar. Davon abgesehen ist in jeder einzelnen Fallgruppe der datenschutzrechtlich begründeten Unlauterkeit zu prüfen, inwieweit sich die UGP-RL auswirkt.

### 4.2. Einfluss der Datenschutzrichtlinien

Darüber hinaus ist iS einer effektiven Durchsetzung des Unionsrechts gleichermaßen zu berücksichtigen, dass die DS-RL nicht bloß einen Mindeststandard für den Datenschutz in der EU schaffen will, sondern auf eine Vollharmonisierung der Rechte der Mitgliedstaaten abzielt und den freien Verkehr personenbezogener Daten im Binnenmarkt zu gewährleisten trachtet.[30] Die Luxemburger Richter räumen zwar ein, dass einige Bestimmungen der DS-RL den Mitgliedstaaten ein Ermessen bei der Umsetzung[31] belassen würden – dazu gehören bspw Art 24 DS-RL, wonach geeignete Sanktionen für Datenschutzverstöße festzulegen sind, und Art 13 DS-RL, der Ausnahmen im öffentlichen Interesse ermöglicht –, andererseits enthalten Art 2 bis 12 DS-RL jedoch sehr genaue Vorgaben darüber, wer wann welche personenbezogenen Daten verarbeiten darf. Dass das Datenschutzrecht (der DS-RL oder eDS-RL) nach Z 26 Anh I der UGP-RL ausdrücklich unbeschadet bleiben soll, bedeutet keinen Ausschluss dieses Rechtsgebiets zugunsten des Lauterkeitsrechts, sondern vielmehr eine ergänzende Anwendung der zum Teil höheren Standards. Ein typisches Beispiel dafür stellt die Regelung des § 107 TKG 2003 gegen unerwünschte Telekommunikation dar.[32]

Als unionsrechtliches Zwischenergebnis ist festzuhalten, dass sowohl das europäische Lauterkeits- als auch Datenschutzrecht jeweils eine Vollharmonisierung anstreben, sodass der Ermessensspielraum der nationalen Gerichte bei der Beurteilung, ob Datenschutzverstöße zugleich als unlauteres Verhalten zu qualifizieren sind, jeweils am Grundsatz des Effet Utile zu orientieren ist, dh dass das Unionsrecht weder in seiner Wirkung noch in seiner Durchsetzung unzulässig beeinträchtigt wird.

### 4.3. Unlauterer Vorsprung durch Datenschutzrechtsbruch

Auch nach Inkrafttreten des UWG 2007 gelten dafür nach der Grundsatzentscheidung[33] des OGH folgende Voraussetzungen, bei deren kumulativen Erfüllung ein Verstoß gegen § 1 Abs 1 Z 1 UWG vorliegt:

- Verstoß gegen generelle Norm
- keine vertretbare Rechtsansicht des Verletzers
- Spürbarkeit des Verstoßes im B2B-Bereich

Ein Verstoß gegen jede – nicht dem Lauterkeitsrecht ieS zuzurechnende – generelle Norm kann eine unlautere Geschäftspraktik oder sonstige unlautere Handlung darstellen, sofern die Auslegung nicht vertretbar ist. Ein solcher Verstoß muss zudem geeignet sein, den Wettbewerb zum Nachteil von Unternehmen nicht nur unerheblich zu beeinflussen (so ausdrücklich § 1 Abs 1 Z 1 UWG).[34] Bei der Beurteilung der Spürbarkeit einer datenschutzrechtlich bedingten Unlauterkeit ist mE danach abzugrenzen, ob die verletzte Vorschrift (bloß) Individualrechte

24) *Aßhoff*, Die wettbewerbsrechtliche Relevanz von Datenschutzverstößen, IPRB 2013, 233; *Linsenbarth/Schiller*, Datenschutz und Lauterkeitsrecht – Ergänzender Schutz bei Verstößen gegen das Datenschutzrecht durch das UWG?, wrp 2013, 576; *Härting/Strubel*, Datenschutz und Wettbewerbsrecht – Die wettbewerbsrechtliche Sanktionierung von Datenschutzverletzungen, IPRB 2011, 231; *Huppertz/Ohrmann*, Wettbewerbsvorteile durch Datenschutzverletzungen?, CR 2011, 449; *Piltz*, Der Like-Button von Facebook – Aus datenschutzrechtlicher Sicht: gefällt mir nicht, CR 2011, 657.

25) Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken – RL-UGP), ABl L 149, 22 ff.

26) EuGH 9. 11. 2010, C-540/08 (Fußballer des Jahres III) Rz 27 = RdW 2010/776, 775 = MR 2010, 347 (*Heidinger*) = wbl 2010/230, 627 = ÖBl-LS 2011/30 = ÖBl 2011/21, 91 = ecolex 2011/62, 142 (*Horak*).

27) Vgl EuGH 4. 10. 2012, C-559/11 (Pelckmans) Rz 24 = ECLI:EU:C:2012:615.

28) EB RV 144 BlgNR XXIII.GP, 9, 3.

29) Vgl EuGH 17. 10. 2013, C-391/12 (Good News) Rz 41 = ecolex 2013, 1134 = wbl 2014/3, 28.

30) EuGH 24. 11. 2011, C-468/10 (ASNEF) = jusIT 2012/29, 68 (*Thiele*); für eine umfassende Harmonisierung bereits *Jahnel*, Datenschutzrecht, Rz 1/38, 1/39; vgl auch EuGH 6. 11. 2003, C-101/01 (Lindqvist) Rz 96 = EuGRZ 2003, 714; 16. 12. 2008, C-524/06 (Huber) Rz 50, 51 = ecolex 2009, 548 = jusIT 2009/52, 109 (*Jahnel*).

31) EuGH 23. 11. 2011, C-468/10, C-469/10 (ASNEF) Rz 52 = jusIT 2012/29, 68 (*Thiele*).

32) Vgl *Knyrim*, Datenschutzrecht², 238 ff mwN.

33) OGH 11. 3. 2008, 4 Ob 225/07b (Stadtrundfahrten) = wbl 2008/137, 290 = MR 2008, 114 = ecolex 2008/199, 551 (*Tonninger*) = RdW 2008/419, 460 = RZ 2008/EÜ 377, 279 = ÖBl-LS 2008/79 = ÖBl 2008/48, 237 (*Mildner*) = SZ 2008/32 = JUS Z/4514 = HS 39.165; dazu *Artmann*, Die Beurteilung der Fallgruppe Rechtsbruch nach der UWG-Novelle 2007, wbl 2008, 253; *Handig*, Subjektive Voraussetzungen im neuen § 1 UWG, RdW 2008, 503; *Heidinger*, Die Fallgruppe Rechtsbruch nach der UWG-Novelle 2007, MR 2008, 108.

34) Vgl *Kraft/Steinmair*, UWG Praxiskommentar (2013) Rz 161 ff.

schützen soll oder potenziell geeignet ist, eine nicht unerhebliche Nachfrageverlagerung zulasten der Mitbewerber zu bewirken. So ist idR eine unvollständige Datenschutzerklärung auf einer Website kein entscheidendes Auswahlkriterium für potenzielle Nutzer, hingegen eine verabsäumte Registrierung oder eine massenhafte Verwendung DSG-widriger Vertragsschablonen sehr wohl spürbar.

#### *4.3.1. Verstoß gegen datenschutzrechtliche Meldeverpflichtungen*

Ein Verstoß gegen jene Normen des DSG 2000, die dem Auftraggeber Melde- bzw Registrierungspflichten auferlegen, ist nach ihrem Zweck einer beabsichtigten Publizität und Transparenz der jeweiligen Datenverarbeitung zum Schutz der Betroffenen, ie der Kunden, Nutzer oder Verbraucher, zu bewerten. Ein Verstoß gegen die Bestimmungen des 4. Abschnitts des DSG 2000 ist dann als unlautere Geschäftspraktik oder als sonstige unlautere Handlung iSv § 1 Abs 1 Z 1 UWG idgF anzusehen, wenn die Norm nicht auch mit guten Gründen in einer Weise ausgelegt werden kann, dass sie dem beanstandeten Verhalten nicht entgegensteht. Das Datenschutzrecht verfügt – ähnlich dem Gewerberecht – über eine ausgeprägte Rechtspraxis der DSB (früher: DSK), beider Gerichtshöfe des Öffentlichen Rechts (VfGH und VwGH) sowie seit 1. 1. 2014 auch des Bundesverwaltungsgerichts. Dazu kommen noch – in rechtsverbindlicher Weise – die Judikate des EuGH. Eine Beantwortung der Vertretbarkeit datenschutzrechtlicher Auslegung hat daher an einem äußerst eng skalierten Maßstab zu erfolgen. Maßgebend sind demzufolge

- der eindeutige Wortlaut und Zweck des Gesetzes unter Berücksichtigung des Anwendungsvorrangs der DS-RL sowie Art 8 GRC einschließlich der EuGH-Rsp,
- die Rsp der Gerichtshöfe des öffentlichen Rechts und des Bundesverwaltungsgerichts sowie
- die beständige Praxis der Datenschutzbehörde.

Die datenschutzrechtlichen Vorschriften, welche die Ausübung einer Tätigkeit bzw die Durchführung einer Datenanwendung, dh automationsunterstützte Datenverarbeitungsprozesse, an bestimmte Voraussetzungen, insb an eine Bewilligung oder Nichtuntersagung knüpfen, dienen regelmäßig auch dem Schutz des lauteren Wettbewerbs. Ihre Übertretung ist daher auch dann unlauter, wenn sie weder fortgesetzt noch planmäßig begangen wurde. Verarbeitet zB ein Laborunternehmen medizinische Daten, ohne dass dafür die datenschutzrechtliche Prüfung und Registrierung nach § 18 Abs 2 Z 1 iVm § 21 DSG 2000 vorliegt, ist diese Vorgehensweise unlauter. Der Laborbetreiber erspart sich einen erheblichen Aufwand, nämlich die Erlangung der Registrierung, und verschafft sich dadurch einen Vorteil gegenüber Mitbewerbern. Der Vorteil liegt nicht nur in einer Kostenersparnis, sondern auch darin, dass das Labor seine Tätigkeit früher aufnehmen konnte als ein eventueller Mitbewerber, der sich an die gesetzlichen Bestimmungen hält und erst nach Vorliegen der Prüfung und Registrierung den Betrieb aufnimmt. Für den rein privaten Bereich haben die Zivilgerichte[35] bereits ausgesprochen, dass die fortdauernde unerwünschte Videoüberwachung von Teilen eines Mehrfamilienhauses durch den Wohnungsberechtigten ohne Meldung an die Datenschutzkommission nicht rechtmäßig und daher nach § 16 iVm § 521 ABGB zu unterlassen ist.

Das DSG 2000 geht nach wie vor vom Grundsatz der Meldepflicht an das Datenverarbeitungsregister (DVR) aus. Ausgenommen von der nach Art 20 DS-RL vorgegebenen Meldepflicht sind nach § 17 DSG 2000 lediglich Datenanwendungen,

- die ausschließlich veröffentlichte Daten oder nur indirekt personenbezogene Daten enthalten,
- die der Führung von gesetzlich vorgesehenen Registern oder Verzeichnissen dienen (zB Personenstandsbücher, Staatsbürgerschaftsevidenz oder das Melderegister),
- die von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten oder für publizistische Tätigkeiten vorgenommen werden, und
- Standardanwendungen: Unter Standardanwendungen (SA) werden Datenanwendungen verstanden, die von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden, wobei eine Gefährdung der Betroffenen unwahrscheinlich ist. In der Zwischenzeit wurde die Verordnung des Bundeskanzlers über Standard-[36] und Musteranwendungen erlassen. Danach zählen etwa Rechnungswesen und Logistik, Personalverwaltung, Mitgliederverwaltung, Kundenbetreuung und Marketing für eigene Zwecke und Aktenverwaltung (Büroautomation) zu den nicht meldepflichtigen Standardanwendungen. Diese Registrierungsfreiheit besteht bei einer Standardanwendung nur, wenn alle Teile der Standardanwendung mit der eigenen Datenanwendung übereinstimmen oder die eigene Datenanwendung zB bei Zweck, Betroffenenkreisen, Datenarten oder den Empfängerkreisen der Übermittlung ein Minus darstellt. Die Personentransport- und Hotelreservierung, Zutrittskontrollsysteme und die KFZ-Zulassung durch beliehene Unternehmen unterliegen als Musteranwendungen (MA) der vereinfachten Meldung. In diesem Fall müssen die Meldungen nur die Bezeichnung der Datenanwendung, die Bezeichnung und Anschrift des Auftraggebers sowie den Nachweis seiner gesetzlichen Zuständigkeit oder rechtlichen Befugnis und die Registernummer des Auftraggebers enthalten, wenn ihm schon eine zugeteilt wurde.

Jede Eintragung beim Datenschutzregister erfolgt für eine bestimmte Datenanwendung, für bestimmte Datenarten, bestimmte Personengruppen und bestimmte Zwecke. Eine DVR-Nummer (siebenstellige Ziffernfolge, zB 0000019) wird einem Unternehmen (Organisation) bei erstmaliger Registrierung einer Datenanwendung nach § 21 DSG 2000 zugeteilt. Die Registrierung (DVR-Nummer) an sich saniert nicht die Rechtmäßigkeit der Datenanwendung im konkreten Einzelfall, sondern betrifft nur die Zulässigkeit der Datenanwendung an sich. Die Registrierung erzeugt keine endgültige Bindungswirkung. Weder die Gerichte noch die Datenschutzbehörde selbst sind letztlich an die Beurteilung der Zulässigkeit im Registrierungsverfahren gebunden. Die Registrierung ist nach § 53 DSG 2000 kostenlos und soll Transparenz sichern, da nach § 16 DSG 2000 jedermann Einsicht in Registrierungen nehmen kann. Dies bedeutet, dass bei registrierungsfreien Datenanwendungen keine DVR-Nummer geführt werden muss.

Alle sonstigen Datenverwendungen, insb die Videoüberwachungen, unterliegen der Meldepflicht, die je nach verarbeiteten/r Daten(art) abgestuft ist. Betrachtet man dieses System, so erscheint aus lauterkeitsrechtlicher Perspektive eine analoge Anwendung jener Grund-

35) Deutlich LG Feldkirch 29. 3. 2011, 2 R 48/11s (Videoüberwachung im Mehrfamilienhaus) = jusIT 2011/88, 182 (*Thiele*) = immolex-LS 2011/61, 197 = MR 2011, 191.

36) BGBl II 312/2004, mehrfach nov, zuletzt mit BGBl II 514/2013.

sätze[37] zutreffend, die zu den gewerberechtlichen Anmelde- und Genehmigungspflichten entwickelt worden sind. Die geschäftliche Relevanz[38] der verabsäumten Meldung iSd § 17 Abs 1 iVm § 19 DSG 2000 liegt auf der Hand: So bestimmt § 18 Abs 1 DSG 2000, dass der Vollbetrieb einer meldepflichtigen Datenanwendung frühestens nach Abgabe der Meldung aufgenommen werden darf. Handelt es sich um eine vorabkontrollpflichtige Datenanwendung, zB bei der Verarbeitung sensibler Daten iSd § 4 Z 2 DSG 2000 oder von Bonitätsdaten, ist selbst nach Erstatten der Meldung eine bescheidmäßige Registrierung der Datenanwendung abzuwarten. Dass es für rechtstreue Reisedienstleister durchaus spürbar ist, uU Monate auf eine Registrierung ihrer Datenanwendungen im Datenverarbeitungsregister (DVR) zu warten, bedarf keiner Erläuterung. Aber selbst im günstigsten Fall des § 18 Abs 1 DSG 2000 müssen gesetzestreue Mitbewerber unter Vorlage diverser Unterlagen (zB FB-Auszug, Gewerbeberechtigung, Dateneingabeformular etc) die Meldung in elektronischer Form im Wege der vom Bundeskanzler bereitzustellenden Internetanwendung einbringen und sich dazu entweder eines Rechtsanwalts oder der eigenen Identifizierung und Authentifizierung durch die Bürgerkarte bedienen.[39]

Abschließend ist zu berücksichtigen, dass die Meldevorschriften iS einer Vorabkontrolle bzw einer Nichtdurchführung vor Ablauf der in § 20 Abs 4 DSG 2000 normierten Zwei-Monats-Frist nicht nur bloße Ordnungsvorschriften darstellen. Die Bekanntgabe der Datenanwendungen *vor* deren Durchführung dient (auch) dazu, die Datenschutzbehörde von Anfang an in die Lage zu versetzen, bereits im Prüfungsverfahren nach §§ 19, 20 DSG 2000 wegen Verdachts der Gefährdung schutzwürdiger Geheimhaltungsinteressen einen sog Mandatsbescheid nach § 22a Abs 4 DSG 2000 zu erlassen, der für Betroffene kaum mehr rückgängig zu machende Privatheitsverluste unverzüglich verhindert, indem die Datenanwendung gestoppt wird. Wird vom Auftraggeber aber erst gar nicht gemeldet, gelangen selbst schwere Datenschutzverstöße – wenn überhaupt – den Behörden eher zufällig und jedenfalls verspätet zur Kenntnis.[40]

### *4.3.2. Verwendung datenschutzgesetzwidriger Auftragsdatenverarbeitung*

Personenbezogene Daten werden in der Praxis teilweise nicht vom Unternehmen selbst, sondern von einem beauftragten Dienstleister, zB Internet Service Provider, Callcenter oder externe Gehaltsabrechner, verwaltet. An der Auftraggebereigenschaft des Unternehmens iSd § 4 Z 4 DSG 2000 ändert sich dadurch zwar nichts, da der Auftraggeber für diese sog datenschutzrechtlichen Dienstleister iSd § 4 Z 5 DSG 2000[41] gegenüber den Betroffenen voll verantwortlich bleibt. § 10 DSG 2000 sieht ausdrücklich die Zulässigkeit derartiger Dienstleister vor, wenn diese Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Dafür sind geeignete Vereinbarungen zu treffen, die zu überprüfen bzw vom Auftraggeber zu überwachen sind.[42] Allein der Abschluss des Vertrages ist nicht ausreichend, um den gesetzlichen Anforderungen Genüge zu tun. Vielmehr muss der Auftraggeber vor Beginn der Datenverarbeitung und dann regelmäßig die Einhaltung der Datenschutzvorschriften beim Dienstleister prüfen bzw sich berichten lassen. Der Mindestinhalt dieser Dienstleisterverträge, dh die Pflichten der Auftragsdatenverarbeitung, sind in § 11 DSG 2000 definiert. Die Verletzung wettbewerbsregelnder Vertragspflichten fällt nach der UWG-Nov 2007 weiterhin unter die lauterkeitsrechtliche Generalklausel iSd § 1 Abs 1 Z 1 UWG. An die Stelle der nach altem Recht erforderlichen Absicht, einen Wettbewerbsvorteil zu erlangen, hat nun die objektive Eignung des Verhaltens zu treten, den Wettbewerb zum Nachteil von rechtstreuen Vertragspartnern nicht bloß unerheblich zu beeinflussen.[43] Verstöße gegen die Grundsätze der Auftragsdatenverarbeitung sind fast immer vorwerfbar, da die gesetzlichen Pflichten sowohl für Auftraggeber als auch Dienstleister sehr klar geregelt sind. Ein Verstoß ist für die Betroffenen idR spürbar, da Zweck der Vorschriften vor allem iZm Bonitätsprüfungen die Transparenz der Datenverarbeitung für Betroffene bildet.[44]

Die bloße Datenüberlassung an Dienstleister ist nach § 4 Z 11 DSG 2000 nicht meldepflichtig.[45] Diese Situation ändert sich allerdings massiv bei der Datenverarbeitung über die Grenze. Grundvoraussetzung für die Zulässigkeit jeder Datenübermittlung ins Ausland ist die Rechtmäßigkeit der Datenanwendung im Inland und die Zulässigkeit der Übermittlung nach den inländischen Vorschriften.[46]

Wenn diese allgemeinen Voraussetzungen vorliegen, ist eine Übermittlung ins Ausland einer Übermittlung innerhalb von Österreich dann gleichgestellt und damit genehmigungsfrei, wenn

- die Übermittlung an Empfänger in Mitgliedstaaten der EU erfolgt oder
- die Übermittlung in Drittstaaten mit angemessenem Datenschutz erfolgt (zB Schweiz und Norwegen).[47]

Ansonsten ist prinzipiell eine *vorherige* Genehmigung der Datenschutzkommission einzuholen. Eine Übermittlung zB von Kundendaten eines österreichischen Textilunternehmens an ein Service-Center in Vietnam ist daher ohne positive Erledigung der Vorabkontrolle unzulässig und auch durch §§ 51, 52 DSG 2000 strafbewehrt. Die bisherige Spruchpraxis[48] der Erteilung von Genehmigungen für den internationalen Datenverkehr gem § 13 DSG 2000 kennt (zahlreiche) Fälle, in denen nach der geltenden Rechtslage Meldungen und Genehmigungen erforderlich sind, bei denen aber eine Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist.[49] Der Gesetzgeber hat daher die Standardanwendung SA033 Übermittlung im Konzern[50] verordnet, die für ganz bestimmte

37) Statt vieler *Schmid* in Wiebe/Kodek, UWG² § 1 Rz 808 ff; jüngst *Barnhouse/Woller*, UWG-Verstoß durch unbefugte Gewerbeausübung, ecolex 2012, 584, jeweils mwN.

38) Vgl *Jahnel/Thiele*, ÖJZ 2004, 870, 872 f (877).

39) Anschaulich *Knyrim/Pawelka*, Datenverarbeitungsregister-Online: Anleitung und erster Erfahrungsbericht, Compliance-Praxis 2013 H 2, 36.

40) Vgl zur anfänglich schlichten Meldung von Google Street View und dem weiteren Verfahren die Darstellung der DSB, abrufbar unter https://www.dsb.gv.at/site/6733/default.aspx (18. 11. 2014).

41) Art 2 lit e DSRL spricht vom Auftragsverarbeiter.

42) Arg „Überzeugen" in § 10 Abs 1 letzter Halbsatz DSG 2000.

43) OGH 11. 5. 2010, 4 Ob 4/10g (Österreichische Auflagenkontrolle II) = wbl 2010/205, 543 = ecolex 2010/403, 1080 (*Tonninger*) = RdW 2010/590, 580. Ein Verstoß gegen § 11 DSG kann daher durchaus eine datenschutzrechtlich geprägte Unlauterkeit zwischen Auftraggeber und Dienstleister begründen, wenn dadurch der Dienstleister dem Auftraggeber Konkurrenz macht oder den Wettbewerb anderer fördert.

44) Vgl VwGH 15. 11. 2012, 2008/17/0096 = jusIT 2013/15, 27 (*Jahnel*).

45) Früh zur begrifflichen Unterscheidung *Jahnel*, Whistleblowing-Hotlines im Datenschutzrecht, ecolex 2009, 1028.

46) Vgl §§ 12, 13 und 55 DSG 2000.

47) Der aktuelle Stand der Länder mit gleichwertigem Schutzniveau findet sich unter http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_de.htm (18. 11. 2014).

48) Vgl zuletzt DSK 30. 9. 2011, K178.414/0006-DSK/2011, RIDA-Nr 0254643; 24. 8. 2011, K178.394/0010-DSK/2011, RIDA-Nr 0255086; 24. 9. 2010, K178.387/0013-DSK/2010, RIDA-Nr 0234837; DSK 25. 4. 2008, K178.298/0004-DSK/2008, RIDA-Nr 0206601.

49) In diese Richtung bereits früh *Knyrim*, Datenschutzrecht (2003) 148 (150).

50) BGBl II 306/2012.

Konzernbereiche[51] die Meldepflicht nach § 17 Abs 2 Z 6 DSG 2000 entfallen lässt.[52]

In den übrigen Fällen stellt eine Missachtung der Vorabkontrolle nach § 13 Abs 1 DSG 2000 einen idR vorwerfbaren und spürbaren Rechtsbruch dar, der geeignet ist, dem Unternehmen einen erheblichen Vorsprung vor dem rechtstreuen Mitbewerber zu verschaffen, weil das behördliche Vorabkontrollverfahren äußerst kosten- und zeitintensiv ist.

#### *4.3.3. Bruch des Datengeheimnisses*

Ein Bruch des Datengeheimnisses nach § 15 DSG 2000 ist gem § 52 Abs 1 Z 2 leg cit mit Verwaltungsstrafe bewehrt und kann auch zu einer strafgerichtlichen Verurteilung nach § 51 DSG 2000 führen.[53] Gerade iZm dem inneren Frontwechsel eines Arbeitnehmers[54] liegt idR ein vorwerfbarer, spürbarer und unlauterer Rechtsbruch vor.

Dabei ist die Beweislastverteilung zu beachten: Steht nämlich nicht (genau) fest, auf welche Weise die beklagten Ex-Beschäftigten in den Besitz der von ihnen verwendeten (wertvollen) Kundendaten der Klägerin gelangt sind, geht dies zu ihren Lasten, weil sie den naheliegenden Verdacht des unredlichen Erwerbs dieser Daten – und damit den Bruch des Datengeheimnisses nach § 15 DSG 2000 – nicht entkräftet haben.[55] Insoweit ist vom Vorliegen eines besonderen, die Unlauterkeit begründenden Umstands iS einer sonstigen unlauteren Handlung iSd § 1 Abs 1 Z 1 UWG auszugehen.

#### *4.3.4. Verwendung datenschutzgesetzwidriger AGB*

Die Datenschutzpraxis stellt exakte Anforderungen an die rechtswirksame Zustimmung Betroffener zur Verarbeitung ihrer personenbezogenen Daten nach § 4 Z 14 DSG 2000. Diese Zustimmung kann auch in Allgemeinen Geschäftsbedingungen (AGB) erteilt werden.[56] Inzwischen besteht dazu eine umfangreiche Klausel-Judikatur der Zivilgerichte, wobei ein Verstoß gegen § 4 Z 4 DSG 2000 bereits zur Gesetzwidrigkeit iSd § 879 ABGB führt.[57]

Nach den bisher in der österreichischen Literatur[58] vorliegenden Stellungnahmen ist die Vereinbarung unzulässiger AGB als (unlautere) Geschäftspraktik iSd § 1 Abs 4 Z 2 UWG zu qualifizieren. Im B2C-Bereich ist die Bestimmung des § 1 Abs 1 Z 2 UWG vorrangig anzuwenden. Die ausschließliche Verwendung unzulässiger AGB gegenüber Unternehmern – wie im Sachverhalt der Zero Intern-Entscheidung – fällt aber unter § 1 Abs 1 Z 1 UWG.[59] Letztlich wird eine freiwillige Harmonisierung der Beurteilungsgrundsätze favorisiert.[60] Die Verwendung datenschutzgesetzwidriger AGB kann daher als sonstige unlautere Handlung iSd § 1 Abs 1 Z 1 UWG qualifiziert werden, wenn keine vertretbare Rechtsansicht vorliegt und dem Verstoß wettbewerbsrechtliche Relevanz zukommt, was idR zu bejahen sein wird.

#### *4.3.5. Informationspflichtverletzung*

Das DSG 2000 enthält – ähnlich dem ECG und dem MedienG – ausdrückliche Informationspflichten für Auftraggeber iSd § 4 Z 4 DSG 2000, die nach § 25 DSG 2000 zu einer Offenlegung der Identität ebenso verpflichten wie zu einer deutlichen Kennzeichnung zB einer Videoüberwachung nach § 50d Abs 1 DSG 2000. Bei meldepflichtigen Datenanwendungen ist nach § 25 Abs 1 DSG 2000 die Registernummer (DVR-Nr) auf den Übermittlungen und Mitteilungen anzugeben. Hauptanwendungsfall der Identifizierungspflicht bei einer Weitergabe bzw Weiterverwendung von Daten nach § 25 Abs 2 DSG 2000 ist die Verwendung von Adressdaten eines Adressverlages zu Werbezwecken eines anderen Unternehmens; beide DVR-Nummern sind anzugeben.[61] Ein Verstoß gegen diese Informationspflichten kann einen unlauteren Rechtsbruch darstellen, der wie eine Impressumspflichtverletzung nach dem ECG oder MedienG zu behandeln ist.

Eine Verletzung der Informationspflicht bei Datenmissbrauch nach § 24 Abs 2a DSG 2000 (sog *Data Breach Notification*)[62] stellt einen besonders schweren Rechtsbruch dar, der idR jedenfalls spürbar ist. Die durch eine EU-VO[63] abgesicherte Aufklärungspflicht gegenüber den Betroffenen und der zuständigen Datenschutzbehörde dient gerade dem Schutz einer breiten Öffentlichkeit vor Schaden durch systematisch und schwerwiegend unrechtmäßig verwendete Daten. Aufgrund der Komplexität der Tatbestandsvoraussetzungen[64] verdient allerdings die Prüfung der Vertretbarkeit einer verspäteten[65] oder einer Nicht-Meldung besondere Beachtung.

### 4.4. Aggressive oder irreführende Geschäftspraktiken

Art 5 UGP-RL stellt das Kernstück der Richtlinie dar und erschließt die Systematik der gesamten Vollharmonisierung durch ein 5-5-4-2-System, dh die Prüfungsreihenfolge

- beginnt mit *Art 5 Abs 5* UGP-RL: Erfüllt ein Verhalten einen der Tatbestände des Anhangs I, ist es jedenfalls unzulässig.
- Erst im zweiten Schritt ist nach Art 5 *Abs 4* UGP-RL festzustellen, ob eine irreführende oder aggressive Geschäftspraktik iSd Art 6 bis 9 UGP-RL vorliegt. Dabei muss das beanstandete Verhalten den Durchschnittsverbraucher zumindest potenziell zu einer geschäftlichen Handlung veranlassen (sog geschäftliches Relevanzkriterium oder Spürbarkeitserfordernis).[66] Es

51) Für die Datenanwendungen Konzernweite Kontakt- und Termindatenbank, Karrieredatenbank, Verwaltung von Bonus- und Beteiligungsprogrammen eines Konzerns und Technische Unterstützung.

52) Näher dazu *Thiele*, Neues zur Datenübermittlung im Konzern, Videoüberwachung & Co – Neuerliche Änderung der Standardanwendung SA032, jusIT 2012, 178 (179).

53) Siehe bereits oben Punkt 1.2.

54) Vgl OGH 22. 5. 2007, 4 Ob 26/07p (Mikrochips) = ECLI:AT:OGH0002:2007:0040OB00026.07P.0522.000, und 18. 6. 2013, 4 Ob 36/13t (Innerer Frontwechsel) = ÖBl-LS 2013/62/66/67/68/69 = wbl 2013/173, 476 = RdW 2013/717, 729.

55) OGH 6. 7. 2004, 4 Ob 147/04b (Flüssiggastanks) = ECLI:AT:OGH0002:2004:0040OB00147.04B.0706.000.

56) OGH 2. 8. 2005, 1 Ob 104/05h.

57) StRsp OGH 24. 7. 2014, 1Ob105/14v (D-Kreditkarten) = ECLI:AT:OGH0002:2014:0010OB00105.14V.0724.000; 14. 11. 2012, 7 Ob 84/12x = jusIT 2013/13, 26 (*Thiele*) = RdW 2013/133, 137 = jusIT 2013/42, 87 (*Forizs*) = RZ 2013/EÜ 186/187/188, 218 = ÖBA 2013, 802 (*Riss*); 22. 6. 2011, 2 Ob 198/10x = jusIT 2011/87, 181 (*Thiele*) = Zak 2012/45, 28 (*Gerhartl*) = RdW 2012/23, 19 = ZVR 2012/92, 166 (*Kathrein*); 22. 4. 2010, 2 Ob 1/09z = jusIT 2010/90, 188 (*Thiele*) = ÖBA 2010, 674 (*Kellner*) = ÖBA 2010/1658, 686 = RdW 2010/643, 627 = SZ 2010/41; 17. 11. 2009, 1 Ob 81/09g = RdW 2010/287, 279 = ÖBA 2010, 304 (*Bollenberger*) = ÖBA 2010/1620, 314 = RdW 2010/480, 422 (*Bollenberger*) = KRES 1d/140; 20. 3. 2007, 4 Ob 221/06p = ecolex 2007/252, 601 (*Wilhelm*) = ÖBA 2007/1450, 981 (*Rummel*) = RdW 2008/10, 53 (*Gehringer*); 13. 9. 2001, 6 Ob 16/01y = JBl 2002, 178 = RdW 2002/67, 79 = ecolex 2002/35, 86 (*Leitner*) = KRES 1h/32.

58) *Heidinger*, Lauterkeitsrechtliche AGB-Kontrolle, Vortrag am 1. Forum Wettbewerbsrecht 25. 11. 2011, zitiert nach *Bauer*, Tagungsbericht, MR 2011, 390 (391); *Schopper*, Die Verwendung unzulässiger Allgemeiner Geschäftsbedingungen als Wettbewerbsverstoß, ecolex 2010, 684 (685); unklar *Schröder*, Gewährleistungsausschluss im Internet – eine rechtsvergleichende Betrachtung, MR 2011, 326 (328); *Thiele*, EuGH bestätigt Unlauterkeit durch gesetzwidrige AGB, RdW 2013, 186.

59) *Thiele*, Zero Intern – Rechtswidrige AGBs als Lauterkeitsverstoß, RdW 2010, 388 (389).

60) *Schröder*, MR 2011, 326 (328 f).

61) Zutreffend *Knyrim*, Datenschutzrecht², 248.

62) Instruktiv *Pachinger*, Datenvorfall – was tun?, ZIR 2013, 244 mwH.

63) VO (EU) 611/2013; dazu *Thiele*, Gesetzgebungsmonitor Datenschutz: VO (EU) 611/2013 in Kraft und DSAV-Novelle 2013, jusIT 2013, 215 mwN.

64) So *Knyrim*, Die neue Data Breach Notification Duty im DSG, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2010 (2010) 59 passim.

65) Vgl § 24 Abs 2a DSG und § 95a Abs 1 TKG 2003, enthalten jeweils „unverzüglich".

66) Vgl EuGH 19. 9. 2013, C-435/11 (CHS Tour Services ./. Team4 Travel) Rz 43 = EC-

liegt eine irreführende oder aggressive Geschäftspraxis aber selbst dann vor, wenn der Unternehmer die berufliche Sorgfalt eingehalten hat.[67]

- Erst die subsidiäre Lauterkeitsprüfung nach Art 5 *Abs 2* UGP-RL führt zu einem unlauteren Verhalten, wenn ein Verstoß gegen die berufliche Sorgfalt zu einer wesentlichen Beeinflussung des wirtschaftlichen Verhaltens eines Durchschnittsverbrauchers geführt haben kann.

Das nationale Lauterkeitsrecht ist daher stets nach dieser Systematik zu strukturieren und zu interpretieren, mag es auch im Weg ungeschriebener Tatbestandsmerkmale erfolgen bzw durch den unionsrechtlichen Anwendungsvorrang zu einem gespaltenen Lauterkeitsrecht kommen. In Fällen, in denen nach Art 5 Abs 5 oder 4 UGP-RL ein unlauteres Verhalten im B2C-Bereich festgestellt worden ist, bleibt die Frage der Erfüllung beruflicher Sorgfaltspflichten allein nach nationalem Recht zur Beurteilung des Verschuldens bei Schadenersatzansprüchen oder für die Annahme einer Wiederholungsgefahr beachtlich.[68]

Die Prüfung der zumindest potenziellen Relevanz des beanstandeten Verhaltens nach Art 5 Abs 4 oder Abs 2 UGP-RL hat im Regelfall nach dem europäischen Verbraucherleitbild des verständigen Verbrauchers[69] zu erfolgen.

Richtet sich jedoch das zu prüfende Verhalten an besonders schutzbedürftige Personengruppen, sieht Art 5 *Abs 3* UGP-RL eine Beurteilung des 5-5-4-2-Systems aus der Perspektive eines durchschnittlichen Mitglieds dieser Gruppe zwingend vor. Spricht daher eine potenziell irreführende Geschäftspraktik objektiv vorhersehbar nur Mitglieder dieser Personengruppe an, so genügt eine Beeinflussung dieser zB besonders leichtgläubigen Verbraucher.

Da der Anh I der UGP-RL bzw der Anh des UWG ausdrücklich keinen Verstoß gegen Datenschutzrecht ieS enthalten, ist auf die Regelbeispiele der Art 6 ff UGP-RL zurückzugreifen. Für Art 6 und 7 sowie 8 und 9 UGP-RL hält die Rsp[70] fest, dass nach diesen Bestimmungen irreführende oder aggressive Geschäftspraktiken verboten sind, wenn sie unter Berücksichtigung ihrer Merkmale und des tatsächlichen Kontexts einen Durchschnittsverbraucher zu einer geschäftlichen Entscheidung veranlassen oder zu veranlassen geeignet sind, die er sonst nicht getroffen hätte. Der EuGH hat also das Verbot solcher Praktiken von keinen anderen als den in diesen Artikeln genannten Kriterien abhängig gemacht.[71] Erfüllt demzufolge eine Geschäftspraxis alle in Art 6 Abs 1 UGP-RL genannten Voraussetzungen für eine Einstufung als den Verbraucher irreführende Praxis (zB eine unzutreffende Exklusivitätsbehauptung), braucht nicht (mehr) geprüft zu werden, ob eine solche Praxis auch den Erfordernissen der beruflichen Sorgfalt iSv Art 5 Abs 2 lit a UGP-RL widerspricht, um sie als unlauter und mithin nach Art 5 Abs 1 UGP-RL verboten ansehen zu können.[72] Art 6 Abs 1 UGP-RL soll wie die Richtlinie selbst ein hohes Verbraucherschutzniveau gewährleisten.

Als aggressive Geschäftspraktik nach § 1a UWG kommt zB eine entgegen § 107 TKG 2003 iVm § 4 Z 14 DSG 2000 vorgenommene belästigende Werbung in Betracht.

Irreführend unlauter ist im Anwendungsbereich des DSG 2000 idR etwa ein Verstoß gegen die Datenverwendung nach Treu und Glauben iSd § 6 leg cit, weil der Betroffene damit über die Umstände des Datengebrauchs und das Bestehen sowie die Durchsetzbarkeit seiner Rechte irregeführt oder im Unklaren gelassen wird.[73] Hervorzuheben ist, dass diese Bestimmung ausdrücklich gem § 48 Abs 1 DSG 2000 auch gegenüber Medieninhabern und deren Mitarbeitern anzuwenden ist.

Schließlich stellt auch die Werbung mit datenschutzrechtlichen Selbstverständlichkeiten – außerhalb von Z 10 Anh UWG – eine sonstige irreführende Geschäftspraktik dar. Dies ist etwa der Fall, wenn ein Unternehmen mit Behauptungen wirbt, wie zB

- *Wir haben unsere Meldepflicht im Datenverarbeitungsregister erfüllt*, wobei volle Registrierungspflicht für die Datenanwendung bestanden hat, oder
- *Wir verpflichten unsere Mitarbeiter auf Ihr Datenschutzgeheimnis*, was ohnehin der gesetzlichen Lage nach § 15 Abs 2 DSG 2000 entspricht, oder
- *Unsere Datensicherheitsmaßnahmen berücksichtigen den Stand der Technik*, was § 14 Abs 2 DSG 2000 für alle Datensicherheitsmaßnahmen der Z 1 bis 8 leg cit verlangt.

In all diesen Fällen besteht eine irreführende Unlauterkeit schon deshalb, weil ein klarstellender Zusatz zur hervorgehobenen Werbeaussage fehlt und beim Verbraucher der unrichtige Eindruck erweckt wird, er erhalte beim werbenden Unternehmen ein höheres Datenschutzniveau als bei der Konkurrenz bzw gesetzlich ohnehin vorgesehen.[74]

### 4.5. Sonstige datenschutzrechtliche Unlauterkeiten

Zu den generellen, nicht dem Lauterkeitsrecht ieS zuzurechnenden Normen nationalen Rechts, die als Ausgangspunkt eines vorwerfbaren Rechtsbruchs dienen können, gehören neben dem normativen Teil eines Kollektivvertrags[75] und sozialversicherungsrechtlichen Gesamtverträgen[76] auch Selbstbindungsnormen der öffentlichen Hand.[77]

Offen ist derzeit, ob auch sog Empfehlungen der Datenschutzbehörde (DSB) gem § 30 Abs 6 DSG 2000 dazu zählen.[78] Diese Empfehlungen stellen das Ergebnis eines weniger formellen Behördenverfahrens nach § 30 DSG 2000[79] dar. Obgleich anlassbezogen, sind Empfehlungen nicht verbindlich. Trotzdem haben sie sich in der Praxis als taugliche Mittel – gewissermaßen pars pro toto – bewährt, um datenschutzrechtliche Verletzungen abzustellen. In einer Empfehlung[80] sprach die Datenschutzkommission (DSK; nunmehr DSB) aus, dass dem Online-Kunden eines Webshops die Möglichkeit gegeben werden muss, das angestrebte Kaufanbot auch ohne die Abgabe der datenschutzrechtlichen Zustimmungserklärung anzunehmen. Eine Einwilligung muss freiwillig

LI:EU:C:2013:574.

67) Vgl EuGH 19. 9. 2013, C-435/11 (CHS Tour Services ./. Team4 Travel) Rz 39 = ECLI:EU:C:2013:574.

68) Deutlich *Musger*, Entscheidungsanmerkung, ÖBl 2014, 22.

69) StRsp seit EuGH 16. 7. 1998, C-210/96 (Gut Springenheide) = ECLI:EU:C:1998:369 = wbl 1998/281 = Ern 1998, 527 = ZER 1998/289.

70) EuGH 23. 4. 2009, C-261/07 (VTB-VAB) Rz 55; 19. 9. 2013, C-435/11 (CHS Tour Services ./. Team4 Travel) Rz 41 = ECLI:EU:C:2013:574.

71) EuGH 19. 9. 2013, C-435/11 (CHS Tour Services ./. Team4 Travel) Rz 41 = ECLI:EU:C:2013:574.

72) EuGH 19. 9. 2013, C-435/11 (CHS Tour Services ./. Team4 Travel) Rz 48 = ECLI:EU:C:2013:574.

73) So ausdrücklich EBRV 1613 BlgNR XX. GP, 39 zu § 6 Abs 1 DSG 2000.

74) Vgl auch BGH 19. 3. 2014, I ZR 185/12 (Geld-Zurück-Garantie III) = GRUR 2014, 1007.

75) OGH 30. 5. 1990, 4 Ob 79/90 (Bankfeiertag) = MR 1990, 196 = ÖBl 1991, 67 = ecolex 1990, 625.

76) OGH 13. 7. 2010, 4 Ob 121/10p (Kassentarif) = ecolex 2010/437, 1172 (*Tonninger*) = ÖBl 2010/50, 264 (*Gamerith*) = RdW 2010/781, 778 = wbl 2011/15, 48 = RdM-LS 2011/28.

77) OGH 12. 3. 1996, 4 Ob 10/96 (Forstpflanzen) = ÖBl 1996, 241 = wbl 1996, 501 = SZ 69/59 = RZ 1997, 115.

78) Instruktiv dazu *Schmidl*, Die Empfehlung gem § 30 Abs 6 DSG 2000, jusIT 2014, 176 mwN.

79) Sog Kontroll- und Ombudsmann; vgl *Schmidl*, jusIT 2014, 176.

80) DSK 13. 7. 2012, K212.766/0010-DSK/2012 = jusIT 2012, 147 (*König*) = RIDA-0265709.

erfolgen. Ist es für den Kunden nämlich nicht möglich, den angestrebten Vertrag mit dem Unternehmen abzuschließen ohne gleichzeitig die in den auf der Bestellwebsite abrufbaren AGB enthaltene Zustimmungserklärung abzugeben, wird dem Erfordernis der Freiwilligkeit iSd § 4 Z 14 und § 8 Abs 1 Z 2 DSG 2000 nicht entsprochen.

Hält sich das konkrete Unternehmen des Anlassfalles nicht daran, kann die DSB eine Strafanzeige erstatten oder Klage vor dem zuständigen Zivilgericht erheben, was aber bislang praktisch nicht vorkommt. Eine allgemeine Verbindlichkeit wird aber durch die Maßnahmen des § 30 Abs 6 Z 1 bis 3 DSG 2000 nicht hergestellt. Aus lauterkeitsrechtlicher Sicht liegt daher mE kein Fall des Rechtsbruchs ieS vor. Dennoch kann ein Verstoß gegen eine Empfehlung der DSB durch ein Branchenmitglied eine unlautere Geschäftspraxis nach § 1 Abs 1 Z 2 UWG darstellen, wenn man den Inhalt der Empfehlung (hier: Trennung von AGB zum Produkterwerb und der datenschutzrechtlichen Einwilligungsklausel) als Maßstab der beruflichen Sorgfalt nach § 1 Abs 4 Z 8 UWG[81] auffasst. Der Begriff der (wettbewerbsrechtlichen) Unlauterkeit wird im Gesetz nicht näher definiert. Nach der Rsp[82] ist dieser Begriff durch Bedachtnahme auf Unternehmer-, Verbraucher- und Allgemeininteressen zu konkretisieren, wobei in § 1 Abs 1 Z 1 UWG die Interessen der Mitbewerber im Vordergrund stehen. Das nach dem Wortlaut nur für § 1 Abs 1 Z 2 UWG maßgebende Erfordernis der Einhaltung der beruflichen Sorgfalt ist auch dem mitbewerberschützenden Tatbestand der Z 1 leg cit zugrunde zu legen.

## 5. Zusammenfassung der Ergebnisse

Die Verfolgung von Datenschutzverstößen als unlautere Geschäftspraktik besitzt einen durchaus erheblichen Anwendungsbereich. Die datenschutzrechtlich geprägte Unlauterkeit verfügt nicht nur über Tradition, wie schon die Rsp zum DSG 1978 und vor der UWG-Nov 2007 gezeigt hat, sondern orientiert sich ganz eng an unionsrechtlichen Vorgaben, die gleichsinnig die Funktionsbedingungen des Leistungswettbewerbs zu verbessern trachten. Dabei werden die Unternehmer-, Verbraucher- und Allgemeininteressen gleichermaßen berücksichtigt.

Verstöße gegen datenschutzrechtliche Meldeverpflichtungen, insb gegen eine Vorabkontrollpflicht nach § 18 Abs 2 DSG 2000 oder im internationalen Datenverkehr nach § 13 DSG 2000 sowie gegen Offenlegungs- (§ 25 DSG 2000) oder Informationspflichten (§ 24 Abs 2a DSG 2000) begründen jeweils einen unlauteren Vorsprung durch Rechtsbruch, dessen Vorwerfbarkeit an der engmaschigen Datenschutzpraxis zu messen und der idR schon aufgrund der Schwere der Missachtung jedenfalls spürbar ist.

Der Bruch des Datengeheimnisses stellt idR eine sonstige unlautere Handlung iSd § 1 Abs 1 Z 1 UWG dar, die mit einer Verletzung von Geschäfts- oder Betriebsgeheimnissen nach § 13 iVm §§ 11, 12 UWG einhergehen kann. Die Verwendung datenschutzgesetzwidriger Zustimmungsklauseln in AGB kann ebenso eine unlautere Geschäftspraktik darstellen wie eine irreführende Werbung mit datenschutzrechtlichen Selbstverständlichkeiten. Schließlich geben Empfehlungen der Datenschutzbehörde nach § 30 Abs 6 DSG 2000 den Maßstab der einzuhaltenden beruflichen Sorgfalt nach § 1 Abs 4 Z 8 UWG wieder.

Verstöße gegen das Datenschutzrecht sind vielfältig und bieten zahlreiche lauterkeitsrechtliche Angriffspunkte. Die Herausforderungen an die Praxis bilden die Vertretbarkeit und die Spürbarkeit einer datenschutzrechtlich bedingten Unlauterkeit, die nur im Einzelfall mit Elan und Entschlossenheit beantwortet werden können. Sie müssen nach den Umständen des Einzelfalls konkretisiert oder präzisiert werden – eine Aufgabe, die der (künftigen) Rsp vorbehalten bleibt.

81) Als eine Art Best-Practice-Standard.

82) Vgl OGH 18. 11. 2008, 4 Ob 185/08x (Logoretusche) = MR 2008, 377 = EvBl 2009/67 = wbl 2009/88, 204 = ecolex 2009/192, 502 (*F. Schuhmacher*) = ÖBl 2009/31, 171 (*Gamerith*) = RZ 2009/EÜ 237, 141 = SZ 2008/167; 5. 7. 2011, 4 Ob 27/11s (Schulschikurse/Exklusivbuchung) = ecolex 2011/366, 933 = wbl 2011/213, 571 = RdW 2011/610, 573 = MR 2011, 329 = RZ 2011/EÜ 217, 284 = ÖBl 2012/17, 61.

Foto D. Wild


**Der Autor:**

RA Hon.-Prof. Dr. *Clemens Thiele*, LL.M. Tax (GGU) studierte US-amerikanisches Steuerrecht in San Francisco; Gründer der RA-Kanzlei EUROLAWYER® in Salzburg; Fachbuch-Autor; Verfasser des Standardkommentars zum RATG[3] (2011); gerichtlich beeideter Sachverständiger für Urheberfragen aller Art, insb Neue Medien und Webdesign.

**Publikationen des Autors:**

Werbeabgabegesetz Kommmentar[2] (2012); Domainmarken – Domain-Namen als Marken, jusIT 2013, 1; gemeinsam mit *Elisabeth Staudegger* Mitherausgeber des Jahrbuchs Geistiges Eigentum 2012, 2013, 2014; Schadenersatz bei vereiteltem Domainpfändung, jusIT 2012, 1; Rechtsgeschäftliche Übertragung von Patenten, RdW 2012, 10; Co-Autor in *Ciresa* (Hrsg), Österreichisches Urheberrecht Kommentar.

**Kontakt:** Anwalt.Thiele@eurolawyer.at