

Hausbesorgerdaten im Internet

OLG Innsbruck 27.9.1999, 1R 143/99k, 28.3.2000, 1 R 30/00x

http://www.eurolawyer.at/pdf/OLG_Innsbruck_1_R_30-00x.pdf

Bei der Klägerin handelt es sich um eine Hausbesorgerin, von der Name, Adresse, Telefonnummer und Zuständigkeitsbereich durch die Beklagte (die Hausverwaltung) im Internet veröffentlicht wurde. Die Klägerin besitzt keinen Internet-Anschluss. Name, Adresse, Telefon und Zuständigkeitsbereich der Hausbesorger werden in die Häusern jeweils an schwarzen Brettern ausgehängt; auch bei Wohnungsübergaben ist die Hausbesorgerin immer anwesend.

Klagebegehren:

Löschung der Daten aus dem Internet.

Begründung: § 43 ABGB (Namensrecht), § 16 ABGB Allgem. (Persönlichkeitsrecht), § 18 DSG 1978 (Datenweitergabe)

Hinweis: Im zweiten Rechtsgang wurde nach (vorbeugend) erfolgter Löschung nur mehr über die Kosten verhandelt. Auch hierbei ist jedoch über die Rechtmäßigkeit der Veröffentlichung zu entscheiden.

Varianten:

1. Es handelt sich um eine "klassische" Mitarbeiterin eines Betriebes von der lediglich die Betriebs-Adresse und die Betriebs-Telefonnummer sowie ihr Aufgabenbereich veröffentlicht wird.
2. Wie Variante 1, aber zusätzlich wird noch ihr Foto veröffentlicht (nur nach Datenschutz untersuchen; Urheberrecht wird hier nicht behandelt!).

Achtung: Entscheidung noch nach dem DSG 1978; in den relevanten Bereichen bestehen jedoch keine Abweichungen.

Verdeckte Videoüberwachung

Deutsches Bundesarbeitsgericht 27.3.2003, AZR 51/02

<http://www.jurathek.de/showdocument.php?ID=6323>

Die Klägerin war Kassiererin in einem Getränkemarkt, dem Beklagten, und dort auch für die Leergutrücknahme zuständig. Hierbei werden die Flaschen entgegengenommen, ein Bon ausgedruckt und mit diesem Bon erhält man dann an der Kasse Bargeld.

In diesem Bereich traten sein 1997 überdurchschnittlich hohe Inventurdifferenzen auf (Geldauszahlungen ohne vorhandenes Leergut). Es erfolgte eine Innenrevision, eine Überprüfung des Warenwirtschaftssystems sowie eine Überprüfung der Arbeitsabläufe. Es blieb jedoch nur mehr absichtliches Fehlverhalten als Grund übrig. Mit diesen Nachforschungen konnte der Kreis der Verdächtigen nicht näher eingegrenzt werden.

Im Jahre 2000 wurde daraufhin versteckt und heimlich eine Videoüberwachung der Kasse durchgeführt, später im Jahr auch in einem angrenzenden Gang, nachdem sich ein Verdacht ergeben hatte. Ob der Betriebsrat der Überwachung zugestimmt hat, wurde nicht festgestellt (gegenläufige Behauptungen). Aufgrund der Videoüberwachung wurde klar, dass die Klägerin Bons ausdrückte ohne Flaschen entgegenzunehmen, mit diesen Bons zur Kasse ging und dort das Geld entnahm. Anschließend begab sie sich damit in den Gang, wo sie das Geld einsteckte.

Darauf hin wurde sie mit Zustimmung des Betriebsrates fristlos entlassen.

Klagebegehren:

Die Klägerin begehrt die Feststellung der Unwirksamkeit der Entlassung und die Nachzahlung des entgangenen Lohnes.

Varianten:

1. Die Videoüberwachung wurde heimlich eingerichtet (Betriebsrats-Zustimmung liegt vor) um eine allgemeine Produktivitätsüberwachung durchzuführen. Hierbei wird zufällig dieser Betrug aufgedeckt. Differiert das Ergebnis?
2. Wie Variante 1, aber diesmal wurde der Betriebsrat nicht befasst (dieser hat keine Kenntnis und daher auch keine Zustimmung abgegeben).

Welche Rechtsfolgen könnte die Videoüberwachung in den Varianten noch hervorrufen?

Friends of Merkur

OGH 27.1.1999, 7 Ob 170/98w

Der Verein für Konsumenteninformation klagt die Merkur AG auf Unterlassung bestimmter (hier kursiver) Klauseln in den AGB's für ein Kundenbindungsprogramm. Hierbei werden persönliche Daten vom Kunden abgefragt. Bei Bezahlung mit der Bankomatkarte, auf welche zusätzliche Daten gespeichert werden, werden besondere Preisreduktionen gewährt.

Beanstandet werden folgende Passagen:

1. M***** behält sich vor, das Kundenprogramm jederzeit ganz oder teilweise zu ändern oder zu beenden. *Veränderte oder ergänzte Konditionen des Kundenprogramms sind für ein Mitglied verbindlich, sobald sie in den M*****-Märkten ausgehängt sind und dem Mitglied die Bezahlung seines Einkaufs mit EC-Karte mit Bankomat-Code tätigt. Eine allfällige Beendigung wird in den M*****-Märkten kundgemacht.*
2. *Ich bin ausdrücklich damit einverstanden, daß meine oben genannten persönlichen Daten EDV-unterstützt verarbeitet und zum Zweck der Konsumenteninformation, sowie allfälliger Werbemaßnahmen an andere Unternehmen des B*****-Konzerns weitergegeben werden.*
3. *M***** trägt keine Haftung für Verlust oder Mißbrauch der EC-Karte, und ist auch nicht in anderer Weise an dem Vertragsverhältnis zwischen Mitglied und seiner Bank beteiligt.*

Die Beklagte führt an, dass das KSchG nicht anwendbar sei, da es sich nicht um ein Austauschverhältnis handle: Der Kunde habe ausschließlich Vorteile durch die Preisreduktion (wegen Teilnahme an dem Programm), ihn treffen aber keine Verpflichtungen. Die AGBs betreffen insbesondere ja nicht die Kaufverträge an den Waren sondern nur das Kundenbindungsprogramm.

Klagebegehren:

Unterlassung der Verwendung der angeführten AGB-Klauseln
Urteilsveröffentlichung in der „Neuen Kronen-Zeitung“

GPS-Überwachung

BGH 4.6.2013, 1 StR 32/13

Der Angeklagte ist Berufsdetektiv und hat im Auftrag von Kunden GPS-Ortungsgaräte an Fahrzeugen angebracht. Diese haben alle ca. 1-2 Minuten Datum, Zeit, Ort und aktuelle Geschwindigkeit per Mobiltelefon übermittelt. Zum Anbringen drang er ihn durch Rolltore, Gitter oder Zugangskarten gesicherte (Tief-)garagen ein. Teilweise wurden mehrere Autos überwacht, die auch von Familienmitgliedern der Überwachten genutzt wurden. Die Daten wurden

in Form von Protokollen und Kartendarstellungen an die Auftraggeber weitergegeben. Folgende Kategorien an Auftraggebern kamen vor:

1. Der Geschäftsführer eines medizinischen Labors ließ überwachen: Angehörige konkurrierender Labore, Personal der Kassenärztlichen Vereinigung Nordbaden (≈GKK), den Insolvenzverwalter seines Vermögens sowie Angehörige der Staatsanwaltschaft die gegen ihn wegen Abrechnungsbetrug ermittelt, um diese anschließend in seinem Sinne beeinflussen zu können.
2. Überwachung von Ehegatten zum Nachweis der Untreue
3. Unternehmen gegenüber seinen Mitarbeitern, die im Verdacht stehen: Hohe Geldbeträge veruntreut und Maschinen unterschlagen zu haben; Verdacht auf Nebentätigkeit im Krankenstand; Spionage für ein Konkurrenzunternehmen
4. Unternehmen zum Auffinden des Arbeitsplatzes einer ehemaligen Mitarbeiterin mit erheblichen Schulden beim Unternehmen.
5. Überwachung der getrennt lebenden Ehefrau wegen Untreue und weil sie ihm „das Haus wegnehmen“ wolle; Überwachung der Ehefrau im Rahmen einer Scheidungsauseinandersetzung.

Keiner der Fälle war schwerwiegend genug, dass die Polizei eine derartige Überwachung hätte durchführen dürfen.

Klagebegehren:

Freispruch vom Vorwurf des vorsätzlichen unbefugten Erhebens von Daten gegen Entgelt (in 29 Fällen + vorsätzlicher Missbrauch von Sendeanlagen durch Verkauf eines Funkscanners zum Abhören eines Telefons: 1,5 Jahre auf Bewährung)

Personendaten im Internet

EuGH, Urteil vom 6.11.2003, Rs C-101/01 („Bodil Lindqvist“)

Frau Lindqvist ist als Katechetin in der Kirchengemeinde Alseda (Schweden) tätig, daneben auch unselbständig als Reinigungskraft. Nach einem Computerkurs richtete sie eine Homepage ein, um Mitglieder der Kirchengemeinde zu informieren. Auf ihren Antrag hin wurde ein Link von der Webseite der schwedischen Kirche auf ihre Webseite erstellt.

Auf den Webseiten waren folgende Informationen über sie und 18 Arbeitskollegen der Gemeinde dargestellt:

- Vollständiger Name oder nur Vorname
- Tätigkeiten und Freizeitbeschäftigungen
- Teilweise die Familienverhältnisse
- Manchmal die Telefonnummer
- Vereinzelt weitere Daten
- Bei einer Kollegin wies sie darauf hin, dass sich diese am Fuß verletzt habe und partiell krankgeschrieben sei

Es wurde keine Zustimmung der Betroffenen eingeholt und die Datenverarbeitung auch nicht bei der Datainspektion (wohl Äquivalent zum DVR) gemeldet. Nach Missbilligung einiger Kollegen wurden die Seiten sofort wieder entfernt.

Die Staatsanwaltschaft leitete ein Verfahren wegen Verletzung folgender Datenschutzvorschriften ein:

1. Automatisierte Verarbeitung personenbezogener Daten ohne vorherige schriftliche Meldung an die Datainspektion
2. Verarbeitung sensibler Daten ohne Genehmigung
3. Übermittlung personenbezogener Daten in ein Drittland ohne Genehmigung

In erster Instanz wurde sie zu ca. € 450 Strafe verurteilt.

Bestehen die Anschuldigungen zu Recht? Konkret war zu entscheiden:

1. Fällt die Nennung einer Person auf einer Webseite unter das Datenschutzrecht? Ist dies eine automatisierte Verarbeitung von Daten?
2. Ist die Angabe der Verletzung am Fuß/Krankschreibung ein „gesundheitsbezogenes Datum“ (=sensible Daten)?
3. Ist die Veröffentlichung im Internet (Schwedische Person stellt schwedische Daten auf schwedischen Server) eine Übermittlung ins Ausland? Kommt es auf die tatsächliche Kenntnisnahme durch Ausländer an? Kommt es auf den Server-Standort an?
4. Sind die Beschränkungen der Richtlinie mit der Meinungsfreiheit/EMRK vereinbar?
5. Kann ein Staat weitergehende Schutzvorschriften erlassen?

Der Sachverhalt ist unbestritten; es geht nur um die rechtliche Würdigung (daher auch eine Entscheidung des EuGH in einem Vorabentscheidungsverfahren!).

Bonitätsauskunfts-Dateien

OGH 1.10.2008, 6 Ob 195/08g

Die Beklagte betreibt eine Auskunft über Kreditverhältnisse. Dafür werden öffentlich zugängliche Bonitätsdaten gesammelt, z.B. über die Ediktsdatei: Exekutionsverfahren. Banken, Versandhändler etc. (ausschließlich Unternehmer) können nach Abschluss eines Vertrages mit der Beklagten auf diese Daten unter Berücksichtigung ihrer AGBs zugreifen. In den AGBs ist festgelegt, dass ein Abruf nur erlaubt ist, wenn der Kunde ein überwiegendes berechtigtes Interesse oder die Zustimmung des Betroffenen nachweisen kann. Eine Bestellung oder eine offene Rechnung reichen als Interessensnachweis aus. Die Informationen dürfen nicht an Dritte weitergegeben oder veröffentlicht werden und sind sofort zu löschen, wenn das Interesse wegfällt. Ob und wie das überwiegende berechnigte Interesse überprüft wird, ist unklar.

Der Kläger wollte einen Mobilfunkvertrag abschließen, welcher ihm jedoch aufgrund der Bonitätsauskunft verweigert wurde. Im Vertragsangebot des Kunden ist angeführt: "Der Kunde erklärt sein ausdrückliches Einverständnis mit der Überprüfung seiner Bonität durch Anfragen bei behördlich zugelassenen Kreditschutzverbänden, Kreditinstituten und Auskunfteien." Daraufhin beantragte der Kläger beim Beklagten die Löschung seiner Daten gem. § 28 Abs 2 DSG 2000, welche abgelehnt wurde.

Klagebegehren:

Löschung der Daten des Klägers aus der Datei

§ 151 Gewerbeordnung

Adressverlage und Direktmarketingunternehmen

(1) Auf die Verwendung von personenbezogenen Daten für Marketingzwecke Dritter durch die zur Ausübung des Gewerbes der Adressverlage und Direktmarketingunternehmen berechtigten Gewerbetreibenden sind die Bestimmungen des DSG 2000 anzuwenden, soweit im Folgenden nicht Besonderes angeordnet ist.

(2) Die Tätigkeit als Mittler zwischen Inhabern und Nutzern von Kunden- und Interessentendateien (Listbroking) ist den in Abs. 1 genannten Gewerbetreibenden vorbehalten.

(3) Die in Abs. 1 genannten Gewerbetreibenden sind berechnigt, für ihre Tätigkeiten gemäß Abs. 1 und 2 Daten aus öffentlich zugänglichen Informationen, durch Befragung der Betroffenen, aus Kunden- und Interessentendateien Dritter oder aus Marketingdateien anderer Adressverlage und Direktmarketingunternehmen zu ermitteln, soweit dies unter Beachtung des Grundsatzes der Verhältnismäßigkeit für

1. die Vorbereitung und Durchführung von Marketingaktionen Dritter einschließlich der Gestaltung und des Versands für Werbemitteln oder

2. das Listbroking

erforderlich und gemäß Abs. 4 und 5 zulässig ist.

(4) Soweit gemäß § 9 DSGVO an sensiblen Daten (§ 4 Z 2 DSGVO) ein schutzwürdiges Geheimhaltungsinteresse besteht, und soweit keine ausdrückliche Zustimmung gemäß § 4 Z 14 DSGVO vorliegt, dürfen sensible Daten von den in Abs. 1 genannten Gewerbetreibenden nur bei Vorliegen der ausdrücklichen Einwilligung des Betroffenen zur Verwendung seiner Daten für Marketingzwecke Dritter verwendet werden. Die Ermittlung und Weiterverwendung von sensiblen Daten aus Kunden- und Interessentendateien Dritter auf Grund einer solchen Einwilligung ist nur im Umfang des Abs. 5 und nur soweit zulässig, als der Inhaber der Datei gegenüber dem Gewerbetreibenden nach Abs. 1 schriftlich unbedenklich erklärt hat, dass die Betroffenen in die Verwendung ihrer Daten für Marketingzwecke Dritter ausdrücklich eingewilligt haben. Strafrechtlich relevante Daten im Sinne des § 8 Abs. 4 DSGVO dürfen von Gewerbetreibenden nach Abs. 1 für Marketingzwecke nur bei Vorliegen einer ausdrücklichen Zustimmung gemäß § 4 Z 14 DSGVO verwendet werden.

(5) Soweit keine Zustimmung der Betroffenen gemäß § 4 Z 14 DSGVO zur Übermittlung ihrer Daten für Marketingzwecke Dritter vorliegt, dürfen die in Abs. 1 genannten Gewerbetreibenden aus einer Kunden- und Interessentendatei eines Dritten nur die Daten

1. Namen,
2. Geschlecht,
3. Titel,
4. akademischer Grad,
5. Anschrift,
6. Geburtsdatum,
7. Berufs-, Branchen- oder Geschäftsbezeichnung und
8. Zugehörigkeit des Betroffenen zu dieser Kunden- und Interessentendatei

ermitteln. Voraussetzung hierfür ist - soweit nicht die strengeren Bestimmungen des Abs. 4 Anwendung finden -, dass der Inhaber der Datei dem Gewerbetreibenden nach Abs. 1 gegenüber schriftlich unbedenklich erklärt hat, dass die Betroffenen in geeigneter Weise über die Möglichkeit informiert wurden, die Übermittlung ihrer Daten für Marketingzwecke Dritter zu untersagen, und dass keine Untersagung erfolgt ist.

(6) Gewerbetreibende nach Abs. 1 dürfen für Marketingzwecke erhobene Marketinginformationen und -klassifikationen, die namentlich bestimmten Personen auf Grund von Marketinganalyseverfahren zugeschrieben werden, nur für Marketingzwecke verwenden und sie insbesondere an Dritte nur dann übermitteln, wenn diese unbedenklich erklären, dass sie diese Analyseergebnisse ausschließlich für Marketingzwecke verwenden werden.

(7) Gewerbetreibende nach Abs. 1 haben Aussendungen im Zuge von Marketingaktionen, die sie mit von ihnen zur Verfügung gestellten oder von ihnen vermittelten Daten durchführen, so zu gestalten, dass durch entsprechende Kennzeichnung des ausgesendeten Werbematerials die Identität der Auftraggeber jener Dateien, mit deren Daten die Werbeaussendung adressiert wurde (Ursprungsdateien), nachvollziehbar ist; soweit Gewerbetreibende nach Abs. 1 an Werbeaussendungen nur durch Zurverfügungstellung oder Vermittlung von Daten mitwirken, haben sie durch entsprechenden Hinweis an die für die Werbeaussendung Verantwortlichen darauf hinzuwirken, dass die Identität der Auftraggeber der benutzten Ursprungsdateien nachvollziehbar ist. Für Gewerbetreibende nach Abs. 1 gilt, wenn sie die Aussendung mit von ihnen zur Verfügung gestellten oder von ihnen vermittelten Daten selbst durchgeführt haben, - unbeschadet ihrer allfälligen Auskunftsverpflichtungen als Auftraggeber -, § 26 DSGVO mit der Maßgabe, dass sie auf Grund eines innerhalb von drei Monaten nach der Werbeaussendung gestellten Auskunftsbegehrens anhand der vom Betroffenen zur Verfügung gestellten Informationen über die Werbeaussendung zur Auskunftserteilung nur über die Auftraggeber der Ursprungsdateien verpflichtet sind; haben sie an der Aussendung nur durch Zurverfügungstellung oder Vermittlung von Daten mitgewirkt, so haben sie nach Möglichkeit zur Auffindung der Auftraggeber der Ursprungsdateien beizutragen. Bei nicht ordnungsgemäßer Erfüllung der Kennzeichnungspflicht durch Gewerbetreibende nach Abs. 1 genügt die Stellung eines fristgerechten Auskunftsbegehrens an den Werbenden zur Wahrung des Auskunftsrechts gegenüber dem Gewerbetreibenden nach Abs. 1.

(8) Stellt der Betroffene an einen Gewerbetreibenden nach Abs. 1 ein Begehren auf Löschung von Daten, die dieser für Zwecke von Marketingaktionen über ihn gespeichert hat, so hat dieser dem Begehren in jedem Fall innerhalb von acht Wochen kostenlos zu entsprechen. Soweit der Betroffene - nach entsprechender Information über die möglichen Folgen einer physischen Löschung seiner Daten - auf der physischen Löschung seiner Daten nicht besteht, hat die Löschung in Form einer Sperrung der Verwendung dieser Daten für Marketingaussendungen zu erfolgen.

(9) Der Fachverband Werbung und Marktkommunikation der Wirtschaftskammer Österreich hat eine Liste zu führen, in welche Personen kostenlos einzutragen sind, die die Zustellung von Werbematerial für sich ausschließen wollen. Die Liste ist mindestens monatlich zu aktualisieren und den Gewerbetreibenden nach Abs. 1 zur Verfügung zu stellen. Gewerbetreibende nach Abs. 1 dürfen an die in dieser Liste eingetragenen Personen keine adressierten Werbemittel versenden oder verteilen und deren Daten auch nicht vermitteln. Die in der Liste ent-

haltenen Daten dürfen ausschließlich zum Zweck des Unterbindens der Zusendung von Werbemitteln verwendet werden.

(10) Inhaber von Kunden- und Interessentendateien dürfen Daten aus diesen Dateien an Gewerbetreibende nach Abs. 1 für Marketingzwecke Dritter nur übermitteln und insbesondere auch für Listbroking nur zur Verfügung stellen, wenn sie die Betroffenen in geeigneter Weise darüber informiert haben, dass sie die Verwendung dieser Daten für Marketingzwecke Dritter untersagen können, und wenn keine Untersagung erfolgt ist; sensible Daten und strafrechtlich relevante Daten dürfen unter den in Abs. 4 genannten Voraussetzungen an Gewerbetreibende nach Abs. 1 übermittelt und für Listbroking zur Verfügung gestellt werden. Auf die Möglichkeit der Untersagung ist ausdrücklich und schriftlich hinzuweisen, wenn Daten schriftlich vom Betroffenen ermittelt werden. Die Untersagung der Übermittlung hat auf ein Vertragsverhältnis zwischen dem Betroffenen und dem Inhaber der Kunden- und Interessentendatei keinen Einfluss.

(11) Jedermann hat das Recht, für sich die Zustellung von adressiertem Werbematerial durch Untersagung der Verwendung seiner Daten für Werbezwecke auszuschließen. Dies kann gegenüber Gewerbetreibenden nach Abs. 1 insbesondere auch durch Eintragung in die im Abs. 9 bezeichnete Liste geschehen.

BGBI.Nr. 194/1994 idF BGBI. I Nr. 42/2008