



WENN MITARBEITER GEHEN, NEHMEN SIE NICHT NUR KNOW-HOW, SONDERN OFT AUCH WICHTIGE KUNDEN MIT. WAS IST GESETZLICH ERLAUBT UND WIE KÖNNEN SICH ARBEITGEBER GEGEN DATENKLAU SCHÜTZEN?

**> Die Inhaberin eines kleinen Friseursalons in einer kleinen Gemeinde im Süden Wiens traute ihren Augen nicht.** Wenige Wochen nach der Kündigung einer Mitarbeiterin zeigten ihr mehrere Stammkundinnen ein Schreiben, das sie von der ehemaligen Mitarbeiterin erhalten hatten: Sie sei ab nun im Salon XY tätig und freue sich auf einen Besuch. Einige Kundinnen berichteten auch von Telefonanrufen, in denen sie das Abwerben neuerlich versuchte und sich nebenbei nicht sehr freundlich über ihre frühere Chefin ausließ. Die Friseurmeisterin stellte selbst

Recherchen an und musste bald feststellen, dass die gekündigte Mitarbeiterin offenbar die Kundendaten aus der Datenbank kopiert und für eigene Werbezwecke verwendet hatte. Mehr als 200 Briefe verschickte sie im gesamten Bezirk mit dem Briefkopf ihres

↖ *Das Abwerben allein ist noch kein Gesetzesverstoß.* ↘

neuen Arbeitgebers, der sich, als er von der Aktion erfuhr, freilich umgehend davon distanzierte.

Viele Unternehmer können von ähnlichen Fällen berichten, mitunter sind die finanziellen Einbrüche durch den Wegfall wichtiger Kunden existenzbedrohend. Nun steht es Kunden prinzipiell frei, mit einem vertrauten Geschäftspartner zur Konkurrenz »mitzugehen« – in Dienstleistungsbranchen ist dies sogar gang und gäbe. Auch den scheidenden Mitarbeitern ist es grundsätzlich nicht verboten, ihr Wissen und ihre Kontakte zu verwerfen. Nicht jede Vorgangsweise ist jedoch rechtlich erlaubt – und in manchen Fällen kann auch der neue Arbeitgeber dadurch einen Rechtsbruch begehen.

**>> Sittenwidriges Verhalten <<**

Das Abwerben von Kunden allein ist noch kein Gesetzesverstoß. Entscheidend ist allerdings, wie der Dienstnehmer an die

## COLD CALLING

➤ Die Kontaktaufnahme mit Kunden ist nicht unproblematisch. Laut Telekommunikationsgesetz (TKG) sind Anrufe bzw. Zusendungen via Fax, E-Mail oder SMS zu Werbezwecken ohne vorherige Einwilligung nicht erlaubt. Bei E-Mails muss die Zustimmung von Endverbrauchern im Fall einer bereits bestehenden Geschäftsbeziehung nicht neuerlich eingeholt werden, wenn die Direktwerbung zu ähnlichen Produkten erfolgt. Zusendungen an Unternehmer bedürfen keiner vorherigen Einwilligung. Allerdings muss den Empfängern in beiden Fällen die Möglichkeit gegeben werden, die Identität des Versenders klar zu erkennen und weitere Nachrichten auszuschließen. Fühlt man sich durch Cold Calling oder Spamming belästigt, kann man bei der Telekommunikationsbehörde ein Verwaltungsverfahren einleiten. Schadenersatz gibt es zwar nicht, die Verwaltungsstrafe kann aber bis zu 38.000 Euro betragen.

Daten gelangt ist und wie er sie verwendet. Die maßgebliche rechtliche Grundlage dafür ist das Gesetz gegen den unlauteren Wettbewerb (UWG). Kundenlisten, insbesondere wenn sie Zusatzinformationen über die jeweiligen Personen enthalten, sowie Geschäftsunterlagen generell zählen als Geschäftsgeheimnis, weil der Arbeitgeber diesbezüglich ein schutzwürdiges Geheimhaltungsinteresse hat. Das gilt auch dann, wenn der Mitarbeiter sie selbst eigenständig oder im Auftrag des Arbeitgebers angelegt hat. Die Grazer Rechtsanwaltskanzlei Likar verweist in diesem Zusammenhang auf ein Urteil des OGH, wonach die Verwertung von

↖ *Der Schaden ist kaum vollständig gut zu machen.* ↘

Geschäftsgeheimnissen noch während eines bestehenden Arbeitsverhältnisses als sittenwidrig erkannt wurde, da der Angestellte »sich nicht mehr als loyaler Mitarbeiter seines Dienstherrn, sondern bereits als dessen künftiger Konkurrent verhielt«.

Der Nachweis des Datendiebstahls ist in der Praxis nicht ganz einfach, insbesondere wenn die Datenbank allgemein zugänglich und nicht durch eigene Passwörter gesichert war. In diesem Fall ließe sich durch technische Mittel eventuell noch nachvollziehen, wer wann auf welche Kundendaten zugegriffen hatte. In Zeiten von Mobile Workspace und Cloud Computing stellen Sperren bzw. der kontrollierte Zugriff auf Kundendaten aber eine der großen Herausforderungen für die Zukunft dar. Denn vielfach haben vor allem Außendienstmitarbeiter ohnehin alle wesentlichen Daten auf ihrem Mobilgerät gespeichert.

### » Aktives Verleiten «

Hat ein Mitarbeiter die wichtigsten Kundenkontakte im Kopf, muss er also keine Liste kopieren oder ausdrucken, ist er rechtlich schwer zu belangen. Mathias Görg, Wettbewerbsrechtsexperte der Kanzlei Maybach Görg Lenneis Geréd Zacherl Rechtsanwälte, berichtet von einem Fall, in dem ein Angestellter letztlich des Datenklaus überführt wurde: »Aufgrund der erforderlichen Detailinformationen gab es nur die Erklärung, dass er sich eine Kundenliste ausgedruckt und hunderte Kunden angeschrieben hatte. Das kann er schlichtweg nicht auswendig gewusst haben.«

Auch der neue Dienstgeber verstößt gegen das UWG, wenn er wissentlich die vom abgeworbenen Mitarbeiter »mitgebrachten« Kundendaten verwendet. Grundsätzlich ist es zwar nicht verwerflich, ehemalige Beschäftigte des Konkurrenzunternehmens herüberzuziehen. Geschieht dies aber mit der Absicht, sich Geschäftsgeheimnisse des Mitbewerbers zu eigen zu machen, verstößt der neue Arbeitgeber gegen das Wettbewerbsrecht. Entsprechendes gilt, wenn er den durch eine Konkurrenzklausele im Dienstvertrag gebundenen Mitarbeiter aktiv zum Vertragsbruch verleitet. Davon, so erklärt Görg, geht die österreichische Rechtsprechung etwa dann aus, »wenn der zukünftige Arbeitgeber die Bezah-

lung einer allfälligen Konventionalstrafe bei Vertragsbruch zusichert«.

Der geschädigte Arbeitgeber kann Schadenersatz verlangen, auch eine Klage auf Unterlassung ist möglich. Sind Kunden unlauter abgeworben worden, kommt auch ein Verbot in Betracht, die betreffenden Kunden weiterhin zu betreuen bzw. sich um weitere Aufträge dieser Kunden zu bewerben. Dennoch: Abgesehen vom hohen finanziellen und emotionalen Aufwand, den gerichtliche Auseinandersetzungen immer nach sich ziehen, ist der entstandene Schaden kaum je vollständig gut zu machen.

### » Exodus der Mitarbeiter «

Besonders unerfreulich wird die Angelegenheit, wenn nicht nur ein Mitarbeiter, sondern gleich ein ganzes Team zur Konkurrenz wechselt, denn dieser massive Verlust von Erfahrungswissen und Detailkenntnissen kann nur begrenzt werden, wenn im Dienstvertrag eine Konkurrenzklausele vereinbart ist. Auch hoch qualifizierte Fachkräfte können auf diese Weise gehindert werden, direkt zum Mitbewerber zu wechseln. Allerdings ist eine solche Klausele u.a. auf maximal ein Jahr begrenzt und darf die Tätigkeit des Arbeitnehmers nicht so stark einschränken, dass dies im Ergebnis einem Berufsverbot gleichkäme.

Für Unternehmen, die auf einen Schlag beispielsweise den Kern ihrer Forschungsabteilung oder ihrer Vertriebsmannschaft verlieren, kann dies zu einer dramatischen Situation führen: Allein um neues Personal zu rekrutieren, sind hohe Investitionen nötig. Und es dauert mitunter Jahre, bis Know-how, Kundenbeziehungen, Einkaufskonditionen und Marktanteile wieder aufgebaut sind.

Experten nennen einen solchen Exodus von Mitarbeitern »Lift-out«. Einer der ersten bekannten Lift-outs ereignete sich nach dem Ende des Zweiten Weltkriegs, als der Luftwaffenoffizier Tex Thornton ein Jobangebot des Autoherstellers Ford nur unter der Bedingung annahm, sein etwa zehnköpfiges Organisationsteam mitnehmen zu dürfen. Die Privatbank Sal. Oppenheim überredete 2005 ein 40-köpfiges Team aus Investmentbankern von Ernst & Young zum Wechsel.

Nicht immer verläuft die Abwerbung reibungslos: Die Preisgabe von firmeninternen Informationen aus dem Umfeld des vormaligen Arbeitgebers kann die Unternehmen in rechtliche Schwierigkeiten bringen. Der Wechsel des Teams um Ignacio López von General Motors zu Volkswagen im Jahr 1983 zog eine juristische Schlacht nach sich, die erst durch Intervention von Bundeskanzler Helmut Kohl und US-Präsident Bill Clinton ein Ende fand. ■

INTERVIEW

# »Einen hundertprozentigen Schutz gibt es nie«

Die Judikatur urteilt hinsichtlich der Wettbewerbsfreiheit zunehmend liberaler, meinen Árpád Geréd und Mathias Görg, Partner bei Maybach Görg Lenneis Geréd Zacherl Rechtsanwälte. Umso wichtiger wird die technische und vertragliche Absicherung für Unternehmen.

24



**MATHIAS GÖRG.** »Der Mitarbeiter darf sich bei der Beschaffung der Daten nicht unlauterer Mittel bedienen.«

**(+) PLUS:** Was ist tatsächlich unzulässig?

**Mathias Görg:** Was das Abwerben von Kunden betrifft, ist das Prinzip der Wettbewerbsfreiheit zu beachten. Ich bin als ehemaliger Mitarbeiter nicht verpflichtet, die Hände in den Schoß zu legen – außer im Dienstvertrag wurde für den betreffenden Geschäftszweig eine wirksame Konkurrenzklausel vereinbart. Der Mitarbeiter darf sich bei der Beschaffung der Daten aber nicht unlauterer Mittel bedienen, also beispielsweise eine Kundenliste mitnehmen. Selbst wenn er diese Kundenliste noch im Auftrag des Arbeitgebers angelegt hat, verstieße eine Mitnahme gegen das UWG. Ausnahme: Er hat die Daten nicht ausgedruckt, sondern im Kopf.



**ÁRPÁD GERÉD.** »Durch die mobilen Endgeräte potenziert sich das Interesse an Fragen betreffend der Sicherheit.«



**Auf welche Daten dürfen alle Mitarbeiter zugreifen?**



**Árpád Geréd:** Ein Verstoß gegen das UWG kann durchaus unangenehme finanzielle Konsequenzen nach sich ziehen. Bei einer Verurteilung habe ich als ehemaliger Dienstgeber einen Veröffentlichungsanspruch und ich kann Schadenersatz verlangen. Hinzu kommen die oft beträchtlichen Prozesskosten. Auch gegenüber den betreffenden Kunden kann sich eine Verurteilung negativ auswirken.

**(+) PLUS:** Wie können sich Unternehmen absichern?

**Geréd:** Überall dort, wo Technologie zum Einsatz kommt, kann man bis zu einem gewissen Grad nachvollziehen, woher Daten stammen bzw. ob und wer Einsicht genommen hat. Mit technischen Maßnahmen kann ich auch Zugriffe beschränken oder verhindern. In der Praxis ist das aber ein komplexes Thema. Vertriebsmitarbeiter sind mit ihren mobilen Geräten ständig unterwegs und haben die Kundenlisten immer mit dabei. In Zeiten des »Cloud Computing« sind alle wunderbar vernetzt und manche Leute wollen auch noch lieber ihre privaten Geräte einbinden, weil sie einen bestimmten Hersteller bevorzugen. All das wollen Unternehmen oft gern ermöglichen. Die Frage, ob der Mitarbeiter mit den Daten womöglich zu einem Konkurrenzunternehmen geht oder ein eigenes Unternehmen aufmacht, wird dabei oft wenig beachtet.

**(+) PLUS:** Wird das Thema Sicherheit an Brisanz zunehmen?

**Geréd:** Auf jeden Fall. Praktisch alle Mitarbeiter haben heute ein Smartphone. Über das E-Mail-Konto synchronisieren sie die Firmendaten. Die Firmenmails sind dann auf dem Gerät und damit auch die Kontaktdaten. Da geht es weniger um Datenschutz, als vielmehr um den eigenen Kundenschutz und den Geschäftsschutz.

Durch die mobilen Endgeräte potenziert sich das Interesse an eigentlich banalen Fragen: Wer darf bestimmte Geräte verwenden? Auf welche Daten dürfen alle, auf welche nur bestimmte Personen zugreifen? Darf wirklich jeder einen USB-Stick anstecken oder ein Smartphone einbinden und Daten herunterladen?

**Görg:** So wichtig die entsprechenden technischen und organisatorischen Vorkehrungen auch sind: Unternehmen ist dringend anzuraten, sich durch entsprechende Klauseln im Vertrag gegen eine Konkurrenzierung so weit wie möglich abzusichern. Einen hundertprozentigen Schutz gibt es aber ohnehin nie.