

## MITARBEITER

## Neue Regeln für geringfügig Beschäftigte

WIEN. Ein Beschäftigungsverhältnis gilt derzeit als geringfügig, wenn das monatliche Entgelt 405,98 € nicht überschreitet. Wird ein Dienstverhältnis für weniger als eine Woche abgeschlossen, dürfen geringfügig Beschäftigte durchschnittlich nicht mehr als 31,17 € pro Arbeitstag verdienen. Ab 2017 wird diese tägliche Geringfügigkeitsgrenze abgeschafft – dies beschloss der Nationalrat im Juni.

„Das ist ein wichtiger Schritt für Arbeitnehmer und Arbeitgeber. Denn so fällt für viele, die nur an wenigen Tagen im Monat arbeiten, die Sozialversicherungspflicht. Und für die Arbeitgeber fällt ein großer administrativer Aufwand weg“, betont Walter Ruck, Präsident der Wirtschaftskammer Wien.

### Handel profitiert

Einen Vorteil bringt die Neuregelung speziell dem Handel oder der Gastronomie. „Gerade da, wo man Kundenkontakt hat, lässt sich der Ansturm und damit der Bedarf an Mitarbeitern schwer abschätzen. Werden Mitarbeiter bisher an einzelnen Tagen aushilfsweise eingesetzt, ist schnell die tägliche Geringfügigkeitsgrenze überschritten“, erklärt Günter Steinlechner, Leiter der Abteilung Sozialpolitik in der Wirtschaftskammer Wien.

Unternehmer müssen für solche Mitarbeiter dann nicht nur Beiträge zur Unfallversicherung zahlen, sondern auch Abgaben wie Kranken- oder Pensionsversicherung. Von der Neuregelung würden auch Pensionisten oder Studenten profitieren, ist Steinlechner überzeugt. Diese können ab 2017 tageweise einer Beschäftigung nachgehen, ohne permanent die Geringfügigkeitsgrenze im Auge zu behalten und andere Ansprüche wie die Pension zu verlieren. [clp]

»claudia.peintner@wirtschaftsblatt.at

## GASTKOMMENTAR

# Geheime Unterlagen in der Cloud

Zunehmend lagern Betriebe Daten in Clouds aus. Dies ermöglicht endlose Speicherkapazitäten und einen weltweiten Zugriff auf Daten. Es ist jedoch ratsam, dass Firmen vom Cloud-Anbieter ein Sicherheitskonzept einfordern.

Stellen Sie sich vor, ein ganzes Team von Mitarbeitern arbeitet an der Konstruktion einer neuen Maschine. Teammitglieder an unterschiedlichen Standorten haben dank der Cloud immer und überall Zugriff auf die jeweils aktuellen Daten und Unterlagen aller anderen Teammitglieder. Klingt gut, aber wie sicher sind die Daten in der Cloud eigentlich? Eine Cloud birgt auch Sicherheitsrisiken, da die endgültige Kontrolle über die Daten aus der Hand gegeben wird. Zum einen hat der Cloud-Betreiber faktisch Zugriff auf alle in der Cloud gespeicherten Daten, andererseits ist das vollständige Löschen der Daten nicht immer garantiert. Außerdem erfolgt der Zugriff über ein Webinterface mittels Passwort. Jeder, der rechtmäßig oder unrechtmäßig in den Besitz des Passworts gelangt, kann sich Zutritt verschaffen.

Das Sicherheitsrisiko beginnt beim physischen Serverstandort, da vor allem bei Public-Cloud-Anbietern der Speicherort der Daten nicht nachvollziehbar ist. Bei der Public Cloud werden die Daten meist auf mehrere unterschiedliche Ressourcenanbieter ausgelagert und an unterschiedlichen Orten gespeichert, etwa in Indien oder den USA.

„Eine 100-prozentige Verfügbarkeit der Cloud ist nicht garantiert.“

**Keine Verfügbarkeit rund um die Uhr.** Unternehmen erwarten eine 100-prozentige Verfügbarkeit der Cloud. Diese ist in den Nutzungsbedingungen aber nicht garantiert. 98 Prozent Verfügbarkeit bedeutet etwa, dass die Cloud insgesamt 7,3 Tage pro Jahr ausfallen darf. Eine Woche ohne Unternehmensdaten – ein Horrorszenario für ein Unternehmen. Noch schlimmer ist wahrscheinlich nur die gänzli-



Cloud Computing bedeutet übersetzt so viel

che Unzugänglichkeit der Cloud, etwa, weil der Anbieter in die Insolvenz schlittert. Unternehmen sollten deshalb eine synchrone Sicherung der Daten auf einem Datenträger außerhalb der Cloud vornehmen, um einen möglichen Schaden aufgrund eines Datenverlusts im Unternehmen zu begrenzen.

Besonders kritisch ist die Auslagerung geheimer oder geschützter Daten. Darunter fallen etwa nach dem Datenschutzgesetz (DSG) geschützte personenbezogene Daten wie Adresslisten, Dienstverträge und sonstige Mitarbeiterdaten, vertraglich geheim zu haltende Unterlagen (z. B. geheime Konstruktionspläne), aber auch gesetzlich geheim zu haltende Daten (z. B. nach dem Anwaltsgeheimnis).

**Haftung für Kundendaten.** Sobald personenbezogene Daten in der Cloud verarbeitet werden, ist das DSGVO maßgeblich. Danach dürfen personenbezogene Daten in der Regel nur mit Zustimmung der Betroffenen in die Public Cloud ausgelagert werden. Gelangen sensible oder geheime Kundendaten wie etwa geheime Konstruktionszeichnungen aus der Cloud in die Hände von Dritten, kann sich das Unternehmen mit Schadenersatzforderungen konfrontiert sehen. Dies gilt vor allem dann, wenn die Sorgfaltspflichten bei der Auswahl des Cloud-Anbieters nicht erfüllt wurden. Grundsätzlich dürfen Unternehmen nur dann einen Cloud-Anbieter für sensible Daten in Anspruch nehmen, wenn dieser ausreichende Gewähr für eine rechtmäßige und sichere Datenanwendung bietet. Empfehlenswert ist daher vorab die Einholung eines Sicherheitskonzepts vom Cloud-Anbieter. Eine Daten-

iStock, beige stellt



wie „Rechnen in der Wolke.“ Unternehmen sollten sich genau ansehen, wem sie ihre Daten in entfernten Rechenzentren anvertrauen.

überlassung ins Ausland ist von der Datenschutzbehörde zu genehmigen, außer wenn einem EWR-Mitgliedsstaat von der Datenschutzbehörde ein angemessenes Datenschutzniveau bescheinigt wurde. Daten dürfen an US-Unternehmen genehmigungsfrei überlassen werden, wenn sich diese den sogenannten „Safe Harbor“-Regeln unterworfen haben.

Unabhängig davon sollten geheime Daten Dritter nicht in eine Public Cloud ausgelagert werden, es sei denn, der Dritte hat der Auslagerung vorab zugestimmt. Eine mögliche Alternative zur Auslagerung geheimer Daten bietet der e-Tresor der A-Trust. Die A-Trust ist eine Gesellschaft im Eigentum der WKÖ, des Rechtsanwaltskammertages, der Notartreuhandbank und anderer Unternehmen aus der Bankbranche. Der Unterschied zur klassischen Cloud liegt im Wesentlichen darin, dass Datenzugriff eine qualifizierte Signatur (Bürgerkarte, Handysignatur) erfordert und die Daten im e-Tresor verschlüsselt werden. Auch kann man ausgewählte Dokumente in einer Showbox durch einfaches Passwort für verschiedene Mitarbeiter zugänglich machen. Aufgrund der Verschlüsselung und der qualifizierten Signatur sind die Daten vor unbefugtem Zugriff besser geschützt und weitgehend sicher.

**GEORG HUBER**

ist Partner der Innsbrucker Rechtsanwaltskanzlei Greiter Pegger Kofler & Partner. Einer seiner Schwerpunkte liegt im IT- und IP-Recht. Der Artikel entstand gemeinsam mit Rechtsanwaltsanwärtin Andreas Schinner.



ANZEIGE

## Gute Berufschancen dank Baulehre

Ch. Ascher

Da die heimische Bauwirtschaft jedes Jahr gut ausgebildete Fachkräfte sucht, bieten sie Jugendlichen eine fundierte Berufsausbildung und gute Aufstiegschancen. Das triale Ausbildungssystem der österreichischen Baulehrlinge ist führend im internationalen Vergleich. Die Lehrlinge lernen im Betrieb, am Lehrbauhof und in der Berufsschule die modernsten Techniken und Entwicklungen der Branche. Damit sind sie nach der Lehrabschlussprüfung als Fachkräfte am Arbeitsmarkt sehr gefragt. Wer sich weiterbilden will, dem stehen außerdem alle Wege offen, den beruflichen Erfolg voranzutreiben. Egal ob Maurer, Schalungsbauer oder Tiefbauer: Mit Fleiß und technischem Ver-



**Innungsmeister Anton Rieder**

ständnis kann jede Fachkraft zum Polier, Vorarbeiter, Werkmeister oder Bauleiter aufsteigen. Auch eine Karriere als Baumeister ist möglich. In Kombination mit der Berufsreifeprüfung können Fachkräfte außerdem die Universität oder Fachhochschule besuchen.

