Whistleblower Wer Missstände aufdeckt, soll künftig stärker geschützt werden. Doch es gibt Widerstand aus der Politik und von Verbänden

Streng geheim

Whistleblower müssen häufig ein enormes Risiko eingehen. Ein Gesetz soll das ändern – manche wittern ein Geschäft

VON KATHARINA KUTSCHE

Hannover – Es ist ein schmaler Grat, den Whistleblower regelmäßig beschreiten. Menschen, die mit einer sinnbildlichen Trillerpfeife auf Missstände hinweisen (engl. to blow the whistle), werden häufig als Denunzianten beschimpft, verlieren ihren Job und ihren Ruf – einmal derart beschädigt, fassen sie nur schwer wieder Fuß in der Gesellschaft und im Arbeitsleben.

Seit Jahren sind Hinweisgeber rechtlich nur schlecht abgesichert. Doch das soll sich spätestens bis Weihnachten ändern. Bis zum 17. Dezember 2021 muss eine EU-Richtlinie in nationales Recht umgesetzt sein, die Whistleblower besser schützt. Das Bundesjustizministerium (BMJV) arbeitet an diesem neuen Hinweisgeberschutzgesetz *(s. Kasten)*. Und weil im September ein neuer Bundestag gewählt wird, soll das Gesetzgebungsverfahren noch in dieser Legislaturperiode abgeschlossen werden, so ein Ministeriumssprecher.

Seinen Verdacht kann der Arbeitnehmer anonym über eine Software melden

Aus diesem Anlass bringen sich ein paar Unternehmen in Position. „Wir sehen einen großen Schub für die Themen Compliance, Ethik und Transparenz“, sagt Achim Weick. Er ist Gründer und Geschäftsführer der Münchner EQS Group. Das Unternehmen entwickelt Meldesysteme, über die Whistleblower Hinweise geben können. „Wir wollen vermitteln, dass es etwas Gutes ist, wenn Missstände aufgedeckt und Mitarbeiter geschützt werden, die sie aufdecken.“

Weick bezieht sich auf einen wesentlichen Punkt in der EU-Richtlinie Nr. 2019/1937. Jener nimmt Arbeitgeber in die Pflicht: Sie müssen zukünftig Hinweisgebersysteme einrichten, über die Beschäftigte Rechtsverstöße melden können. Das gilt, so die Umsetzungsplanung des BMJV, für bestimmte Dienststellen sowie Unternehmen mit mindestens 250 Mitarbeitern, von 2023 an auch für solche mit mindestens 50.

Hinter diesen Systemen verbergen sich spezielle IT-Programme mit Dialogfunktion. Fällt etwa einem Arbeitnehmer auf, dass in seiner Abteilung etwas schiefläuft, zum Beispiel ein Vorgesetzter Schmiergelder kassiert, kann er den Verdacht anonym über die Software melden. Die Person auf der Gegenseite kann offene Fragen klären und um Belege bitten. Am Ende wird der Verdacht erhärtet oder eben nicht.

Bisher aber haben sich Firmen oft schwergetan mit solchen Verfahren. Weick kennt die üblichen Vorurteile und Sorgen: zu viele Meldungen ohne Substanz, zu viele verleumderische Meldungen und überhaupt zu viele Meldungen. Ein Kunde aus dem Mittelstand habe ebenfalls diese Ängste artikuliert, bevor er das EQS-Produkt einsetzte: Tatsächlich aber gingen nur drei Meldungen im ersten Jahr ein – und die waren alle sehr relevant, erzählt Weick. „Hinweise über ein Meldesystem können den Schaden für Unternehmen begrenzen – ich verstehe nicht, warum sich manche Firmen dagegen wehren.“

Jene, die sich wehren, fürchten meist, dass ihr Image durch Vorwürfe und Verdachtsmomente beschädigt wird. Dabei übersehen sie, dass sie es bei einer internen Meldung selbst in der Hand haben, den Schaden zu begrenzen.

Klar ist: Arbeitnehmer sind gegenüber ihrem Arbeitgeber grundsätzlich zur Loyalität verpflichtet. Sie haben aber auch ein Recht auf Meinungsfreiheit. Und dann ist da noch das gesellschaftliche Interesse daran, Missstände aufzuklären und zu beseitigen. In dieser Gemengelage war es bisher vor allem das deutsche Arbeitsrecht, das sich mit Fällen von Whistleblowing beschäftigte. Dabei ging es immer auch um die Frage, mit welchem Kenntnisstand und bei wem sich ein Hinweisgeber meldet: erst intern? Oder gleich an die Öffentlichkeit gehen?

Wenn es etwa um Korruption geht, werden rund ein Viertel der Ermittlungsverfahren von bekannten oder anonymen Hinweisgebern angestoßen. Das ergibt sich aus dem Lagebild des Bundeskriminalamtes für 2019. Die Behörde führt darin auch aus, dass insgesamt gut die Hälfte aller Verfahren ihren Ursprung in polizeiexternen Quellen habe. Was die Bedeutung qualifizierter Hinweise für eine erfolgreiche Korruptionsbekämpfung unterstreiche.

Bisher gilt, dass Arbeitnehmer nicht gekündigt werden dürfen, wenn sie zuerst innerhalb ihres Betriebs anzeigen, was ihnen aufgefallen ist – sie müssen dabei „in gutem Glauben“ handeln. Im neuen Hinweisgeberschutzgesetz soll nun in § 7 festgeschrieben werden, dass Beschäftigte wählen können, ob sie sich an eine interne oder eine externe Meldestelle wenden. Arbeitgeber sollen zwar Anreize dafür schaffen, dass sich Hinweisgeber zuerst intern melden, aber die „Möglichkeit einer externen Meldung darf hierdurch nicht beschränkt oder erschwert werden“.

Bei den gängigen Systemen ist das technisch kein Problem, sie können so eingerichtet werden, dass sie etwa in der Rechtsabteilung einer Firma oder extern bei einer Ombudsperson landen. Das Meldesystem, das EQS selbst nutzt, leitet Hinweise in die Fachabteilungen – so müsse niemand Sorge haben, dass die Chefetage Unbequemes unterdrückt. Acht Meldungen habe es im eigenen Laden gegeben, sagt Weick, zwei davon nicht relevant, keine missbräuchlich. Bei den gemeldeten Fällen geht es übrigens nicht nur um Korruption oder andere Wirtschaftsstraftaten. Eine Mitarbeiterin habe sich nach einer Feier belästigt gefühlt und den Vorfall über die Software gemeldet, erzählt Weick. Das Unternehmen handelte, der beschuldigte Mitarbeiter habe das Unternehmen verlassen.

Weick, 52, kommt ursprünglich aus dem Investmentbanking und gründete 2000 die EQS. 2005 übernahm die Firma die Deutsche Gesellschaft für Ad-hoc-Publizität (DGAP), einen Meldepflichtendienst für börsennotierte Unternehmen. Das Thema Whistleblowing ist seit 2018 im Portfolio: EQS kaufte Integrity Line, eine Schweizer Firma aus Zürich. Inzwischen hat die Gruppe rund 800 Kunden, elf Standorte weltweit und rund 450 Mitarbeiterinnen und Mitarbeiter. „Wir können glaubhaft rüberbringen, dass wir für Transparenz stehen. Wir sind selbst börsennotiert und müssen viele Regularien einhalten. Und wir wissen, wie man das effizient umsetzt“, sagt Weick.

Viele große Unternehmen nutzen die Software von EQS bereits, darunter die Europäische Zentralbank und Continental. Doch in Europa gebe es an die 50 000 Unternehmen mit mehr als 52 Mitarbeitern, sagt der Gründer, eine Menge potenzielle neue Kunden also. Er hofft auf einen Marktanteil von 20 Prozent und die europäische Marktführerschaft.

Da hat aber noch der Pionier auf dem Gebiet mitzureden: Business Keeper. Das Berliner Unternehmen ist seit 2003 auf dem Markt. Sein erster Kunde war das Landeskriminalamt Niedersachsen, inzwischen nutzen etwa auch das Bundeskartellamt, die Deutsche Bahn oder die Österreichische Nationalbank das System von Business Keeper. Kai Leisering, 54, der seit 2008 die Geschäfte bei Business Keeper führt, schaut mit einer gewissen Skepsis auf die EU-Richtlinie. „Aus der Sicht eines Geschäftsführers finde ich das wunderbar. Es bringt uns neue Kunden, das merken wir schon seit vergangenem Jahr“, sagt Leisering. 2020 habe das Unternehmen 20 neue Mitarbeiter fest angestellt. Als Privatperson bezweifle er aber, dass ein Hinweisgebersystem in kleineren Unternehmen eine Wirkung entfaltet.

Wenn ein Anbieter gehackt würde, wäre das ein Problem für das Ansehen der ganzen Branche

Vor allem stört ihn, dass mit der neuen Regelung neue Anbieter wie Pilze aus dem Boden schießen, die auf ein gutes Geschäft hoffen. „Wir sind auch ein Wirtschaftsunternehmen, aber aus einer ethischen Motivation heraus entstanden.“ Gründer Kenan Tur habe Business Keeper aufgebaut, um „werteorientiertes Wirtschaften“ zu unterstützen. Daher sei die große Sorge des Unternehmens der Schutz der Hinweisgeber. „Wir investieren jedes Jahr viele Hunderttausend Euro in IT-Sicherheit. Das können die kleinen Anbieter noch nicht“, sagt Kai Leisering. „Und wer dann gehackt wird, hat ein Problem: Das würde sich auf die gesamte Vertrauenskultur von Hinweisgebersystemen auswirken und auch Haftungsrisiken für Anbieter und Nutzer nach sich ziehen.“

Wer das Vertrauen von Whistleblowern gewinnen will, muss ihnen glaubhaft Anonymität zusichern können. Business Keeper wirbt daher schon seit Langem damit, dass das Unternehmen selbst auf Druck von Behörden nicht in der Lage wäre, die Identität von Hinweisgebern herauszufinden. „Wir lassen es uns von unabhängigen Stellen regelmäßig zertifizieren, dass wir Hinweise technisch nicht nachvollziehen können.“

Das ist aus Sicht von Leisering auch ein wesentlicher Punkt, den Kunden bei der Suche nach einem Anbieter berücksichtigen sollten: „Anonymität ist nicht das Gleiche wie Verschlüsselung.“ Wenn ein Unternehmen damit werbe, sein System sei auf einer Cloud, also einem zentralen Speicherort im Internet aufgesetzt, kann das zum Problem werden. Die größten Cloud-Plattformen wie Amazon Web Services oder Microsoft Azure, sind US-Firmen. Und nach dem Cloud-Act gesetzlich verpflichtet, US-Behörden Daten herauszugeben, die von Kunden in der Cloud gespeichert wurden, unabhängig davon, wo die Server stehen. So würde ein Hinweisgebersystem ad absurdum geführt.