VON KERSTIN BLOSSEY,
BLOSSEY & PARTNER

Whistleblowing – was geht's mich an?

Schwierigkeitsgrad:

"Whistleblowing" ist ein Begriff, den es im Grunde seit Menschengedenk gibt, der aber erst um die Jahrtausendwende richtig salonfähig zu werden begann. Überall dort, wo es um Korruption oder Verschwendung in staatlichen oder privatwirtschaftlichen Organisationen geht, wo es um Fragen der Umwelt, des Gesundheits- oder Verbraucherschutzes sowie um die Sicherheit von Produktionsanlagen und gefahrenträchtige Einrichtungen geht, finden wir das Lebensumfeld des Whistleblowers.

IN DIESEM ARTIKEL ERFAHREN SIE...

- Was Whistleblowing ist,
- Wo Whistleblowingsysteme am Arbeitsplatz eine Rolle spielen,
- Warum es wichtig ist, solche System sensibel einzurichten.

WAS SIE VORHER WISSEN/KÖNNEN SOLLTEN...

Keine spezifischen Vorkenntnisse erforderlich, die Grundbegriffe des Datenschutzes aus den Artikeln der vorherigen Ausgaben sollten geläufig sein. Alternativ kann auf das Glossar von Blossey & Partner (*http://blossey-partner.de/showpage.php?SiteID=11&lang=1*) zurückgegriffen werden.

Er schlägt Alarm, wo Gefahren und Risiken oder bereits entstandene Schäden bagatellisiert werden, wo effektive Vorschriften gezielt unterdrückt oder umgangen werden, wo Gesetzesverstöße und Straftaten ungeahndet bleiben, wo betriebsinterne Missstände ignoriert oder Risiken in Wissenschaft, Forschung und Technik verschwiegen werden. Whistleblowing wird zunehmend öffentlich diskutiert und bewegt. Auch Fachzeitschriften widmen diesem Begriff immer mehr Aufmerksamkeit. Seit 1999 wird sogar der „Whistleblower-Preis" in Deutschland verliehen.

Kennzeichen von Whistleblowing

Die „Pfeife blasen" – was Whistleblowing im wörtlich übersetzten Sinn heißt – meint zunächst das „Enthüllen gravierender Missstände". Der Whistleblower oder etwas schlicht eingedeutscht „Hinweisgeber" (*Anm. d. Autorin: ich verzichte auch in diesem Artikel auf die Unterscheidung weiblicher und männlicher Schreibweise zugunsten der Lesbarkeit*) deckt grobes Fehlverhalten und Fehlentwicklungen in seinem Arbeitsumfeld oder Wirkungskreis auf. Für gewöhnlich handelt der Whistleblower aus ethischen Maßstäben heraus und riskiert damit nicht nur seinen Arbeitsplatz – und damit seine Existenzgrundlage - sondern unter Umständen auch sein soziales Netzwerk und seine Reputation.

Er wird deshalb den Alarm zunächst im persönlichen oder beruflichen Rahmen schlagen („internes Whistleblowing"). Hat er damit nicht den erforderlichen Erfolg, z. B. weil seine entsprechenden Hinweise gezielt unterdrückt werden, wird sich der Whistleblower normalerweise an die Öffentlichkeit wenden, etwa an entsprechende Aufsichtsbehörden, Gewerkschaften, Berufsverbände, Journalisten und Massenmedien („externes Whistleblowing"), um schwerwiegende Folgen aufgrund der Missstände verhindern zu helfen. Da er seinem Umfeld nicht selbst Schaden zufügen, sondern einen solchen zu erwartenden Schaden verhindern möchte, wird er den Weg nach außen tunlichst vermeiden, wenn möglich. Der Whistleblower agiert also uneigennützig und orientiert sich nicht an persönlichen (auch wirtschaftlichen) Vorteilen. So viel zur Theorie.

Whistleblowing am Arbeitsplatz

Beschäftigten, die am Arbeitsplatz Alarm schlagen, wird oft zunächst vorgeworfen, dass sie arbeitsvertragliche Pflichten verletzen, ihnen wird Illoyalität und Schädigung des Betriebsklimas vorgeworfen. Meist ist Whistleblowing mit der Preisgabe vertraulicher innerbetrieblicher Informationen verbunden, die dem Unternehmen nachhaltig Schaden

zufügen können. Hier liegen die Hürden des Whistleblowers, und er ist herausgefordert, sein Vorgehen genau abzuwägen und schließlich eine klare Linie zu gehen. Sein Vorgehen ist eben nicht dadurch geprägt, dass er, wie ein Denunziant, manipulierend richtige oder falsche Informationen verbreitet und Verleumdungen, Beleidigungen und falsche Verdächtigungen in die Öffentlichkeit trägt. Der Whistleblower ist darauf bedacht, eine unabhängige Aufklärung erkannter Missstände anzustrengen, wo bestimmte Machtverhältnisse versuchen, dies zu verhindern. Während Whistleblower Unternehmensleitung und Unternehmenseigentümern helfen, Missstände im Unternehmen frühzeitig zu erkennen, gilt es im Kontext des demokratischen Diskurses, die Autoritätsgläubigkeit abzulegen und einen neuen Umgang mit Kritik und Fehlern auf allen Hierarchieebenen zu erlernen, denn Whistleblowing ist weit mehr als schlicht ausgedrückt eine Art Korruptionsbekämpfung.

Immer mehr Unternehmen – gerade in den USA – orientieren sich in ihrer Unternehmensführung an Werten wie Ehrlichkeit, Vertrauen, Integrität und Fairness und vereinen diese Werte in ihrem „Code of Ethics“ oder „Code of Conduct“. Um diesen Gewicht zu verleihen, bedarf es eines Selbstkontrollsystems wie Whistleblowing als einer wertvollen betrieblichen Ressource. Längst wurde auch in Deutschland erkannt, dass eine effektive und produktive Unternehmensführung ohne moralische und ethische Werte nur bedingt möglich ist. Whistleblowing, ob intern oder extern, kann dafür sorgen, dass jenes Vertrauen in die Seriosität eines Unternehmens für die Gesellschaft ebenso wie für die eigene Belegschaft verifizierbar wird.

Hauptgrund für die zunehmende Salonfähigkeit des Whistleblowings dürfte aber sicherlich der so genannte „Sarbanes-Oxley Act“ sein, der 2002 aufgrund der zunehmenden Bilanzskandale erlassen wurde, um die Verlässlichkeit der Berichterstattung von Unternehmen zu verbessern, die an der US-Börse notiert sind. Gemäß US-Bundesgesetz sind US-Unternehmen schlicht zur Einrichtung eines Whistleblowing-Systems verpflichtet, um Korruption und Betrug aufzudecken. Hiervon sind auch europäische Unternehmen betroffen, sofern sie über die bundesdeutschen Grenzen hinaus auf dem US-Börsenmarkt aktiv werden wollen.

Das „Hinweisgeben“ wird also zunehmend fester Bestandteil der Gesellschaft und der Unternehmenskultur – und damit des Managements in der Privatwirtschaft und allen weiteren Organisationsformen. Hier wird Whistleblowing internes Kontrollverfahren verstanden, das Verfahren zur Meldung von Missständen anbietet. Immer mehr Unternehmen richten eine Compliance-Management-Abteilung ein, die selbst verantwortlich dafür Sorge zu tragen hat, dass die Einhaltung aller Vorgaben durch die Rechtsordnung, die Unternehmensleitung und das Personal gewährleistet ist. Primäres Ziel des Compliance-Manager/-Officer ist es, der Bildung eines Negativimage entgegen zu wirken, sowie Haftungsfälle und Schadensersatzklagen bestmöglich auszuschließen.

Spätestens wenn man Whistleblowing als das praktizierte Recht auf freie Meinungsäußerung nach Artikel 5 Grundgesetz verstehen will, wird klar, dass der Schutz eines solchen „Hinweisgebers“ eine zentrale Rolle im System spielen muss.

Datenschutz

Zumeist wendet sich jener Mitarbeiter, der Missstände in seinem Arbeitsumfeld erkennt, an die Compliance-Abteilung. Um die Meldung sachlich und – vor allem zum Schutz des Whistleblowers – weitgehend anonym zu halten, nutzen einige Unternehmen firmeninterne Telefonhotlines oder ein entsprechendes externes Angebot diverser namhafter Unternehmensberatungsgesellschaften, die hier eine Marktlücke für sich entdeckt haben.

Gilt es, eine angemessene Funktionsweise der Organisation bzw. Unternehmung zu sichern, ist die Erhebung und Nutzung personenbezogener Daten gemäß § 28 Absatz 1 Satz 2 Bundesdatenschutzgesetz (BDSG) und Artikel 7 Buchstabe C der Datenschutzrichtlinie 95/46/EG zulässig, wenn sie, unter Wahrung möglicherweise schutzwürdiger Interessen des Betroffenen, der Wahrung berechtigter Interessen der verantwortlichen Stelle dient. Bei der Erfassung personenbezogener Daten ist der jeweilige Geschäftszweck konkret festzulegen, zum Beispiel als „im Sinne des geordneten und wirtschaftlich erfolgreichen Ablaufs des Wertschöpfungssystems erforderliches Instrument“. In diesem Rahmen, also etwa zur Aufklärung eines konkreten Verdachtsmoments mit entsprechend hoher Verhältnismäßigkeit, ist die Erhebung personenbezogener Daten im Rahmen mit bestehenden Gesetzen zulässig. Die Verhältnismäßigkeit ist regelmäßig als gegeben anzusehen bei Hinweisen zu Straftaten und massiven Pflichtverletzungen, insbesondere zu Missständen in den Bereichen Rechnungslegung, interne Rechnungslegungskontrolle, Wirtschaftsprüfung und Bekämpfung von Korruption.

Nach Artikel 17 der Richtlinie 95/46/EG muss das Unternehmen,

Wochenrückblick zu den Datenschutz-Schlagzeilen in der Online-Presse:

Das Redaktionsteam von Blossey & Partner stellt jede Woche neu die Schwerpunktthemen rund um Datenschutz für Sie zusammen unter *http://www.blossey-partner.de* („News“, unten rechts). Gucken Sie doch mal rein, das Archiv reicht inzwischen bis 2005 zurück und bietet sogar eine Suchfunktion. Viel Spaß beim Stöbern.

das für ein System zur Meldung von Missständen verantwortlich ist, die geeigneten technischen und organisatorischen Maßnahmen im Sinne des § 9 BDSG und Anlage zu § 9 BDSG treffen, die für die Gewährleistung der Sicherheit der Daten bei ihrer Erhebung, Verbreitung, Speicherung und Weitergabe erforderlich sind. Ziel ist dabei, die Daten gegen die zufällige oder unrechtmäßige Zerstörung sowie gegen Verlust, unberechtigte Weitergabe oder den unbefugten Zugriff zu schützen. Es muss also in der Praxis zum Beispiel gewährleistet sein, dass Meldungen nicht unbefugt (erst recht nicht zufällig!) von Dritten gelesen werden können. Wirksame Maßnahmen könnten hier eine angemessene Form der Datenverschlüsselung oder auch eine restriktive Zugriffskontrolle mittels einem durchgängigen hierarchieübergreifenden Rollen- und Berechtigungskonzept sein.

Gemäß Artikel 11 der Richtlinie 95/46/EG sind die betroffenen Personen zu unterrichten, wenn personenbezogene Daten bei Dritten erhoben werden (vgl. § 33 Abs. 1 S. 1 BDSG). Die Benachrichtigungspflicht entfällt jedoch, wenn die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle gefährden würde (§ 33 Abs. 2 Nr. 7 BDSG). Der Geschäftszweck ist hier die Aufklärung des Straftatverdachts, deren Gefährdung durch die Benachrichtigung zu bejahen ist. Nach Einstellung oder Abschluss der Ermittlungen müssen die Daten unverzüglich und in der Regel innerhalb von zwei Monaten irreversibel gelöscht werden (vgl. § 35 Abs. 2 Nr. 3 BDSG).

Wird ein ausgelagertes Whistleblowingsystem verwendet, gelten zusätzlich die Anforderungen an die Auswahl von und die vertragliche Gestaltung der Zusammenarbeit mit dem entsprechenden externen Dienstleister im Sinne des § 11 BDSG. Nur so kann sichergestellt werden, dass Informationen über den Hinweisgeber nicht in unbefugte Hände geraten und dann missbraucht werden können. In diesem Punkt besteht gerade in deutschen Unternehmen oft ein großes Defizit. Vertragliche Ergänzungsvereinbarungen beispielsweise wären in der Praxis leicht machbar, jedoch scheuen viele Firmen die – in fast allen Fällen unbegründete! – Gefahr, sich bei dem jeweiligen Geschäftspartner unbeliebt zu machen.

Natürlich stellen die genannten Aspekte noch keine vollständige Liste aller zu treffender Datenschutzmaßnahmen bezüglich eines Hinweisgebersystems dar. Eine solche Aufstellung bedarf der sorgfältigen Analyse eines praxiserfahrenen Datenschutz-Profis, der sowohl die Interessen des Unternehmens als auch die schutzwürdigen Belange der betroffenen Menschen ausreichend berücksichtigen kann. Entsprechend angemessene Maßnahmen können auch dann nur im Team mit den Fachleuten der beteiligten Abteilungen entwickeln werden. Die Angemessenheit ist jedoch ein nicht zu unterschätzender Faktor, wenn es um die Einhaltung entsprechend geschaffener Regelungen – und damit wiederum um die Betroffenen – geht.

Informantenschutz

Generell sollte das Unternehmen selbst für einen angemessenen Schutz von Hinweisgebern sorgen. Hierfür bieten sich Personalvertretung bzw. Betriebsrat in Form einer entsprechenden Vereinbarung zum Schutz Betroffener und der Whistleblower ebenso wie zur Vertretung der Unternehmensinteressen an.

2003 schaffte das Bundesarbeitsgericht mit seinem Urteil eine Art Kündigungsschutz für Angestellte, indem es festlegte, dass der Angestellte, der Strafanzeige gegen einen Vorgesetzten aufgrund von gravierenden Missständen stellte, eine Kündigung nur dann befürchten muss, wenn er unwahre Angaben macht (BAG 03.07.2003 – 2 AZR 235/02).

Wie teuer ein Informant tatsächlich bezahlen muss, wenn er dabei an die falsche Adresse gerät, zeigen diverse Beispiele von Mobbing, Kündigung und Schlimmerem, wenn man genauer hinsieht, so erzählt von einem ehemaligen Controller Im Manager Magazin im Juni 2008 [1]. Die Internationale Handelskammer (ICC) hat im selben Jahr als mutmaßlich erste Organisation der Weltwirtschaft Richtlinien zum Whistleblowing veröffentlicht, die - als globaler Standard eingeführt – bei der Einrichtung entsprechender Programme in Unternehmen und Einrichtungen hilfreich sein könnten [2].

Nachdenkliches Fazit: Zivilcourage versus Bespitzelungssystem?

Die Deutschen sind – neben der Qualität ihrer Arbeit und Produkte – auch bekannt für ihre Streitlust vor Gericht. Für einen Prozess reicht oft schon ein über den Zaun hängender Ostbaumast. Analog zu dieser Streitbarkeit und im Begriff der Überlegung, dass der Reigen der „langen Wellen“ nach Kondratieff [3] sich nicht nur auf die Konjunktur, sondern genauso gut auf alle Abläufe der Geschichte der Menschheit gleichermaßen beziehen könnte, kann man leicht zu dem Schluss kommen, dass sich ein System von Whistleblowern früher oder später im Reigen der Kondratieffzyklen zu einem tragfähigen Netz von Misstrauen und Verrat bis in die eigene individuelle Sozialstruktur entwickeln könnte. Schon allein vor diesem – ich gebe zu sehr persönlichen – Hintergrund betrachtet, ist eine sorgfältige Abwägung des Wie und Weshalb für die Einführung eines Whistleblowingsystems in einem Unternehmen dringen zu empfehlen. Besonders, wenn die für die Frankfurter Fairness-Stiftung vom Baseler Entwicklungssoziologe und Whistleblowing-Experte Klaus Leisinger erstellte Definition zutrifft: Whistleblower sind "Menschen, die sich - zunächst auf dem Dienstweg, dann aber auch dezidiert außerhalb desselben - bemerkbar machen. Sie weisen auf illegale oder - aus ihrer Sicht - illegitime Handlungsweisen einer Person, eines Unternehmens, einer Partei, einer Gewerkschaft, einer Kirche oder einer anderen Institution hin" [4]. Letztlich liegt es wohl zu gleichen teilen in der gesellschaftlichen und

Verwendete Quellen:

- *http://www.manager-magazin.de/magazin/artikel/0,2828,562441,00.html*
- *[2] http://www.icc-deutschland.de/fileadmin/ICC_Dokumente/GuideICCWhistleblowing.pdf*
- *[3] Nefiodow Leo A. - Der sechste Kondratieff: Wege zur Produktivität und Vollbeschäftigung im Zeitalter der Information. Die langen Wellen der Konjunktur und ihre Basisinnovation, Rhein-Sieg Verlag, Sankt Augustin 20004; ISBN 3-980-51445-5;*
- *[4] brand eins online - http://www.fairness-stiftung.de/Presseauswahl.asp?PSNr=31 (Stand: 6/2003);*
- *[5] Orwell G. – 1984, Ullstein Tb; ISBN 3-548-23410-0;*
- *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; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html*
- *Gola, Schomerus – BDSG-Kommentar, § 28, 16a, Verlag C. H. Beck, München 20079; ISBN 3-406-55544-6;*
- *Simitis S. - Bundesdatenschutzgesetz, Nomos Verlagsgesellschaft, Baden-Baden 20066; ISBN 3-832-91376-9;*
- *Humanistische Union e.V. - Innere Sicherheit als Gefahr, Berlin 2002;*
- *Whistleblower Netzwerk e.V. - http://www.whistleblower-net.de/ (Stand: 06.07.2009);*

unternehmerischen Verantwortung, geeignete Lösungsmöglichkeiten zu suchen und zu finden, die dafür sorgen, dass aus einem sinnvollen Kontrollsystem gegen massive Formen von Korruption, Betrug und Geschäftsschädigung keine moderne Form der Bespitzelung durch ein (wie in Georg Orwells „1984" skizziertem [5]) Netz von Denunziation werden kann.

Zur Autorin

Kerstin Blossey ist Dipl. Informations-Wirtin (FH) und Gründerin von Blossey & Partner, einem aufstrebenden Unternehmen, das sich ganz auf den betrieblichen/behördlichen Datenschutz spezialisiert hat. Zum Kundenkreis zählen deutsche wie international angesiedelte mittelständische Unternehmen, Konzerne und Einrichtungen aus so unterschiedlichen Branchen wie Telekommunikation, Medien & Presse, Softwareindustrie, Automotive, Wirtschaft, Gesundheitswesen, Tourismus und der öffentlichen Hand.