Herausforderungen bei der Implementierung von Hinweisgebersystemen

Im Spannungsfeld zwischen Whistleblower- und Datenschutz

Der Fall Edward Snowden hat dem Thema „Whistleblowing" nochmals einen Schub gegeben. Immer mehr Unternehmen beschäftigen sich proaktiv mit der Implementierung sogenannter Hinweisgebersysteme, denn die NSA-Affäre hat auch gezeigt, welche Schäden von einer Meldung ausgehen können, die in die Öffentlichkeit getragen wird.

Von Kenan Tur, Berlin

Ohne ein eigenes adäquates, vertrauensbildendes System steigt nicht nur das Haftungsrisiko, es besteht auch die Gefahr, dass vertrauliche Interna, etwa auf Leak-Plattformen oder in sozialen Netzwerken veröffentlicht werden. Unternehmen und Verwaltungen setzen daher interne Whistleblowing-Systeme ein,um sowohl monetäre als auch reputative Schäden abzuwenden. Darüber hinaus können diese Systeme auch eine positive Innenwirkung entwickeln und – eingebettet in das Compliance-Management-System – dazu beitragen, ein Klima von Transparenz und Vertrauen zu fördern. Dabei sollten sie – sofern gewünscht – die Anonymität der Hinweisgeber gewährleisten können.

Einer aktuellen Studie von PwC und der Universität Halle-Wittenberg zufolge[1] verfügen nur knapp 40% der befragten deutschen Unternehmen über ein Hinweisgebersystem, obwohl Studien immer wieder die Relevanz interner Meldungen zu Missständen und Fehlverhalten[2] belegen. Indes ist ein zunehmendes Interesse insbesondere größerer Unternehmen an derartigen Anwendungen zu registrieren. Mittlere Unternehmen ziehen nach, denn auch sie sind immer öfter gezwungen, auf Compliance-Entsprechungserklärungen der Konzerne oder Lieferanten-Audits zu reagieren.

Wie verschiedene Beispiele in den vergangenen Jahren gezeigt haben, verursachen Korruptionsvorfälle nicht nur monetären, sondern insbesondere auch reputativen Schaden für die Unternehmen. Unsere Erfahrungen belegen, dass sich die unmittelbaren finanziellen Konsequenzen, inklusive der Auswirkungen auf den Aktienkurs, meist sehr viel kurzfristiger negativ auf den Unternehmenserfolg auswirken als der entstandene Imageschaden. Auch die negativen Einflüsse auf die Unternehmenskultur und die Mitarbeitermotivation sind häufig noch lange Zeit spürbar.

Eine wichtige Voraussetzung für den effizienten Einsatz von Hinweisgebersystemen ist, dass sich die Geschäftsleitung mit den Anforderungen an die Umsetzung auseinandergesetzt hat und sich auch entsprechend verpflichtet fühlt, allen Hinweisen verantwortungsbewusst nachzugehen. Unternehmen und Verwaltungen sollten daher bereits vorab ihren genauen Bedarf in Bezug auf das gewünschte Hinweisgebersystem formulieren.

Die Systeme

Welches Hinweisgebersystem zum Einsatz kommt, hängt von der Unternehmensstruktur, der potenziellen Hinweisgebergruppe sowie der Systemausgestaltung (unternehmensinterne Lösung vs. Einbeziehung von Externen) ab. Denkbar sind grundsätzlich vier Varianten: Der Brief, sprachbasierte Systeme wie etwa Telefonhotlines, Ombudsleute und internetbasierte Anwendungen. Auch Kombinationen sind möglich.

Der Brief fungiert auch heute noch als niedrigschwelliges, zeit- und ortsunabhängiges Instrument der Hinweisübermittlung, das jedoch schnell zu einer kommunikativen Einbahnstraße werden kann, wenn der Hinweisgeber anonym meldet.

Telefonhotlines stellen ebenfalls einen niedrigschwelligen Kommunikationskanal dar – allerdings genießen sie wenig Vertrauen hinsichtlich der Anonymitätswahrung. Um eine 24-h-Erreichbarkeit zu gewährleisten und international agierenden Unternehmen eine entsprechende Sprachenvielfalt anbieten zu können, sind für deren Betrieb zudem große personelle Ressourcen notwendig. Kostengünstigere Anrufbeantworter bergen hingegen ein hohes Risiko für unvollständig übermittelte Informationen. Zudem haben sie den Nachteil, dass erst zeitverzögert auf einen Hinweis reagiert werden kann. Bei rein E-Mail-basierten Systemen ist ähnlich den Hotlines das Vertrauen in den Datenschutz eher gering.

Der Einsatz einer internen Vertrauensperson, eines Compliance Officers oder externen Ombudsmanns ermöglicht eine Selektion der Themen, zu denen gemeldet werden kann. Zudem eröffnet ein Dialog überhaupt erst die Möglichkeit, Nachfragen zur Klärung des Sachverhalts zu stellen und eine Glaubwürdigkeitsprüfung durchzuführen. In Bezug auf die Sprachenvielfalt sowie die zeitliche und örtliche Verfügbarkeit sind diese Lösungen hingegen naturgemäß beschränkt. Sie werden daher meist im regionalen Kontext eingesetzt.

Internetbasierte Systeme

Vermehrt kommen heute internetbasierte Hinweisgebersysteme zum Einsatz, da sie ohne die Nachteile anderer Anwendungen auskommen. Hierbei muss zwischen rein HTML-basierten

Lösungen und in sich abgeschlossen programmierten Applikationen (Software-Anwendungen) differenziert werden, die erst die nötige Sicherheit vor dem Zugriff unberechtigter Dritter gewährleisten können. Hervorzuheben ist, dass sie rund um die Uhr, weltweit und in jeder möglichen Sprache zur Verfügung gestellt werden können und nur eines geringen personellen Aufwands bedürfen. Durch spezielle Verschlüsselungsverfahren kann sowohl die Anonymität des Hinweisgebers als auch die Sicherheit der erhobenen Daten gewährleistet werden. Auch für den Fall, dass der Hinweisgeber seine Identität zunächst nicht preisgeben möchte, ist es möglich, über spezielle Funktionen[3] einen sicheren Dialog mit dem Bearbeiter anzubieten, der Rückfragen und eine Plausibilitätsprüfung zulässt. Ein an das System gekoppeltes „Case Management" zur systematischen Fallbearbeitung ermöglicht zudem die rechts- und revisionssichere Dokumentation der Fallbearbeitung sowie die sofortige Auskunftsbereitschaft sowohl gegenüber externen Aufsichtsorganen als auch den internen Kontrollgremien. Über Filtermechanismen bieten internetbasierte Systeme die Möglichkeit, bestimmte Meldungsthemen auszuschließen, etwa Delikte nach §138 StGB 3, bei denen eine Meldepflicht an deutsche Strafverfolgungsbehörden besteht und eine Unterlassung der Meldung strafbar ist.[4]

Mit der Kombination eines solchen Systems und einer Ombudsperson oder auch einer Telefonhotline können darüber hinaus Hinweisgeber erreicht werden, die das Gespräch mit einer Kontaktperson bevorzugen sowie jene, die lieber „aus sicherer Distanz" über den Computer kommunizieren. Bei international eingesetzten Ombudsleuten muss in manchen Ländern (etwa in Entwicklungs- und Schwellenländern) zu deren Schutz jedoch das Zeugnisverweigerungsrecht sichergestellt sein. Hinzu kommen kulturelle Besonderheiten: So wenden sich nach unserer Erfahrung potenzielle Hinweisgeber in Ländern, in denen viele unterschiedliche Ethnien leben (etwa in Indien oder in Afghanistan), unter Umständen nicht an eine Kontaktperson, die einer anderen ethnischen Gruppe angehört.

Bei der Entwicklungshilfe hat man aus den Erfahrungen der vergangenen Jahrzehnte gelernt und setzt in den jeweiligen Ländern heute gezielt Ansprechpartner und Vermittler mit unterschiedlichem ethnischen oder religiösen Hintergrund ein. Unternehmen, die den Einsatz von Ombudsleuten in mehreren Ländern planen, sind sich der Anforderungen in Anbetracht der interkulturellen Vielfalt häufig jedoch nicht bewusst.

Internationale Gesetze

Bei länderübergreifend eingesetzten internetbasierten Hinweisgebersystemen sind die Datenschutzanforderungen des jeweiligen Landes zu beachten und die zu erfassenden Meldungsschwerpunkte entsprechend den dort gegebenen Anforderungen und Möglichkeiten zu prüfen. Diese länderspezifischen Anforderungen müssen sowohl bei der Implementierung als auch bei der technischen Umsetzung (Customizing) berücksichtigt werden. Zu beachten ist etwa, dass:

- in einigen Ländern nur eine namentliche Meldung zulässig ist (zum Beispiel in Portugal).
- datenschutzrechtliche Vorschriften gegebenenfalls die Auswahl der Themen einschränken sowie auch über welche Personengruppe (abhängig von deren Position) im Unternehmen gemeldet werden darf (zum Beispiel in Schweden).
- die Identität des Whistleblowers nur ausgewählten Personen oder Instanzen bekannt bleiben soll (etwa bei Anzeige einer Vorteilsannahme im Betrieb). Hinweisgeber wünschen sich erfahrungsgemäß, dass ihre Identität nur einer Person oder einem sehr kleinen Personenkreis bekannt ist.
- eine Aufdeckung der Identität des Hinweisgebers durch Rückverfolgung soziale oder gar lebensbedrohliche Folgen haben kann. Die Angst von Hinweisgebern vor Repressalien ist nicht unbegründet. Während in Mitteleuropa eher die Angst vor dem Verlust des Arbeitsplatzes im Vordergrund steht, ist in anderen Ländern nicht selten auch das Leben des Hinweisgebers bedroht. Aus lateinamerikanischen, afrikanischen und einigen asiatischen Ländern wurde von mehreren Fällen berichtet, in denen die Familie des Hinweisgebers ermordet wurde, um andere potentielle Hinweisgeber abzuschrecken.
- der Kreis der auf die Meldung zugreifenden Bearbeiter eindeutig definiert und beschränkt ist – zudem müssen alle Beteiligten über den vorgegebenen Bearbeitungsablauf in Kenntnis gesetzt werden.
- in manchen Ländern ein Hinweisgebersystem bei der jeweiligen Datenschutzbehörde angemeldet werden muss (zum Beispiel in Österreich oder Frankreich).

Auch in Europa gibt es einen dringenden Bedarf für die Regelung des Schutzes von Hinweisgebern. So kommt der Bericht „Whistleblowing in Europe. Legal Protection for Whistleblowers in the EU"[5] von Transparency International, der die rechtlichen Rahmenbedingungen in 27 EU-Mitgliedstaaten untersucht, zu dem Ergebnis, dass nur vier Länder – Großbritannien, Luxemburg, Rumänien und Slowenien – über einen guten Schutz verfügen. Deutschland befindet sich im unrühmlichen Mittelfeld. Auch hierzulande sollte sichergestellt werden, dass Mitarbeiter ohne Angst vor arbeitsrechtlichen oder anderen Konsequenzen eine Meldung zu potenziell strafrechtlichen Vorkommnissen abgeben können und sich – im Wissen geschützt zu sein – auch an Stellen außerhalb des Unternehmens wenden können, wenn der internen Meldung nicht nachgegangen wird. Andererseits belegen Studien, dass mehr als 90% der Hinweisgeber das Unternehmen nach Bekanntwerden ihrer Identität verlassen, weil sie sich von Kollegen ausgegrenzt fühlen.

Betriebsrat miteinbeziehen

Zu empfehlen ist, auch mit dem Betriebsrat (wenn vorhanden) eine Vereinbarung abzuschließen, die den Umgang und den Einsatz des Systems ▶

1 www.pwc.de/de/risiko-management/wirtschaftskriminalitaet-2013.jhtml
2 ACFE 2012 „Report to the Nations on Occupational Fraud and Abuse" www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf
3 etwa die Postkastenfunktion des BKMS-System. Details hierzu unter www.business-keeper.com/whistleblowing-compliance.html. Das System besitzt zudem das ULD-Datenschutzsiegel sowie das EuroPriSe-Siegel.
4 s. etwa https://de.wikipedia.org/wiki/Nichtanzeige_geplanter_Straftaten
5 www.transparency.org/whatwedo/pub/whistleblowing_in_europe_legal_protections_for_whistleblowers_in_the_eu

Besonderheiten durch US-Vorgaben

Vor dem Hintergrund der NSA-Affäre ist die Situation deutscher Unternehmen mit US-Bezug besonders interessant. Die EU-Richtlinie 95/46/EG verbietet es grundsätzlich, personenbezogene Daten aus EU-Mitgliedsstaaten in Staaten zu übertragen, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auf die USA zu, da diese keine umfassenden gesetzlichen Regelungen kennen, die den Standards der EU entsprechen. Zwar wurde nachträglich das sogenannte Safe-Harbor-Abkommen abgeschlossen, dass es europäischen Unternehmen ermöglicht, personenbezogene Daten legal in die USA zu übermitteln, allerdings handelt es sich hierbei nicht um einen verbindlichen völkerrechtlichen Vertrag.US–Unternehmen können sich jedoch auf freiwilliger Basis verpflichten, den Anforderungen des Abkommens zu entsprechen. Der 2002 verabschiedete Sarbanes–Oxley Act, der für Unternehmen und deren Tochterunternehmen gilt, die an US–amerikanischen Börsen gelistet sind, fordert explizit ein anonym nutzbares Hinweisgebersystem in Bezug auf fragliche Rechnungslegungs– oder Wirtschaftsprüfungsangelegenheiten. Bei Nichteinhaltung der Vorschrift kann die US–Börsenaufsichtsbehörde verschiedene Sanktionsmaßnahmen ergreifen – bis hin zu einer Aussetzung des Handels der jeweiligen Wertpapiere. Vor dem Hintergrund, dass Hinweisgebersysteme einerseits datenschutzrelevante Daten beinhalten können und andererseits potenziell strafrechtlich relevante Aktivitäten beschreiben werden, ist es nicht unkritisch, dass der US-PATRIOT Act den Strafverfolgungsbehörden weitreichende Zugriffsrechte auf Daten einräumt.

Auch Server in Europa können keinen sicheren Schutz vor Zugriff aus den USA gewährleisten, da die Instandhaltungs- und Sicherungsarbeiten zumeist vom jeweiligen US-Dienstleister erbracht werden, der muss die Vorgaben der US-Bundesbehörden einhalten. Dies birgt für Unternehmen Risiken, die sie beim Aufsetzen ihres Hinweisgebersystems, der Wahl des Server-Standortes und der Datenhaltung berücksichtigen sollten. Dieser Sachverhalt zeigt, welche Bedeutung es für deutsche Unternehmen hat, die Daten in Europa, besser noch in Deutschland, zu speichern – ohne Zugriffsmöglichkeiten durch US-Dienstleister und US-Behörden.

regelt. In Deutschland existiert dazu zwar keine rechtliche Verpflichtung, jedoch sollte dies als Teil der Organisationseinheit eines Unternehmens einbezogen werden. Diskussionsbedarf besteht meist in Bezug auf die Auswahl der Themenschwerpunkte, zu denen Hinweise erfasst werden sollen. Hierbei achtet der Betriebsrat insbesondere darauf, dass keine Verhaltenskontrolle der Mitarbeiter im Zuge des Einsatzes eines Systems stattfinden kann. Erfahrungen zeigen auch, dass die Sorge vor denunziatorisch motiviertem Missbrauch in Unternehmen zwar weit verbreitet, aber nahezu unbegründet ist, da Hinweisgeber in der Regel vor allem aus ethisch-moralischen Beweggründen handeln.

Technik für die Anonymität

Hinsichtlich der Frage, wie moderne, internetbasierte Whistleblowing-Systeme im nationalen und internationalen Einsatz die geforderte Anonymität bei der Übermittlung garantieren können ist festzuhalten, dass sich heute prinzipiell jede Verschlüsselung umgehen lässt. Aus diesem Grund gilt es umso mehr, den Aufwand für Angreifer bei der Übermittlung der Hinweise entsprechend zu erhöhen. Bewährt haben sich zu diesem Zweck asymmetrische Kryptoverfahren, die von unabhängigen Sachverständigen begutachtet und zertifiziert sein sollten. Auch regelmäßige Penetrationstests durch Spezialisten erhöhen die Sicherheit. Als Konsequenz aus der NSA-Affäre ist es ratsam, die Daten ausschließlich auf geschützten Servern in Deutschland zu speichern. Dritte, darunter auch die Anbieter der Hinweisgebersysteme selbst, sollten dabei zu keinem Zeitpunkt Zugriff auf die verschlüsselt abgespeicherten Meldungen haben. Darüber hinaus müssen sich moderne Hinweisgebersysteme unterschiedlichen länderspezifischen rechtlichen Normen anpassen können, wie etwa den oben genannten Datenschutzvorschriften.

Es gibt Aufbewahrungsfristen, die eingehalten werden müssen. Unabhängig vom gewählten System sollte das Löschen der Daten aus datenschutzrechtlichen Gründen immer möglich sein. Wenn Meldungen nicht plausibel sind oder sich ein Verdacht nach einer erfolgten Prüfung nicht bestätigt, sind diese in Deutschland ohnehin nach dem BDSG (Bundesdatenschutzgesetz) innerhalb von zwei Monaten zu löschen. Andere Löschfristen existieren, wenn in den Meldungen keine personenbezogenen Daten angegeben wurden. Auch hier sind zudem die jeweiligen länderspezifischen Gesetzesvorgaben zu beachten.

Fazit

Unternehmen profitieren davon, mit einem umfassenden Werte- und Compliance-Management die Voraussetzungen zu schaffen, strafrechtlich relevanten Vorfällen bereits präventiv entgegenzuwirken bzw. diese zumindest intern aufklären zu können. Als essentieller Bestandteil eines modernen Compliance-Management-Systems sollten Hinweisgebersysteme den jeweiligen Anforderungen in den Unternehmen flexibel angepasst werden. Die Akzeptanz des Systems seitens der Mitarbeiter sowie deren Vertrauen in den Umgang mit den übermittelten Hinweisen sind entscheidend für die Effizienz der Anwendung. Dazu bedarf es eines mit der Implementierung des Systems beginnenden und kontinuierlich weitergeführten Kommunikationsplans. Ziel sollte sein, alle Beteiligten sowohl über den Nutzen des gewählten Systems als auch über dessen Anwendung zu informieren. Hierfür bieten sich unterschiedliche Kommunikationswege an, etwa Mitarbeiterzeitschriften, der Arbeitsvertrag, das Intranet oder Newsletter. Bei global agierenden Unternehmen sollte diese Kommunikationsstrategie länderspezifische Gegebenheiten nicht nur in sprachlicher Hinsicht berücksichtigen, sondern auch unter Bezugnahme auf die kulturelle Vielfalt des jeweiligen Landes. Auch müssen die Rahmenbedingungen der betrieblichen Mitbestimmung und des Datenschutzes beachtet werden. Auf EU-Ebene haben sich hierzu unabhängige Stellen zur Zertifizierung von Dienstleistungen oder IT-Produkten in Übereinstimmung mit dem europäischen Datenschutzrecht etabliert, etwa die Prüfstelle für das European Privacy Seal (EuroPriSe).

Nicht zuletzt gilt es, den Schutz für Hinweisgeber zu regeln. Ihnen sollte eine sichere, auf Wunsch anonyme, Meldungsabgabe stets möglich sein. Es hat sich gezeigt, dass viele Hinweisgeber, die zunächst ohne Angabe ihres Namens melden, ihre Identität im Laufe des Dialogs preisgeben, weil sie Vertrauen zum Bearbeiter gefasst haben. Ohne die Möglichkeit zur anonymen Kontaktaufnahme wäre der Hinweis jedoch vermutlich ausgeblieben.

Über unseren Autor:

Kenan Tur ist Diplom-Wirtschaftsinformatiker und war bei General Motors in verantwortlicher Position im strategischen Einkauf tätig. Sein Interesse an dem Thema Wirtschaftsethik inspirierten ihn zur Entwicklung eines in sich geschlossen programmierten elektronischen Hinweisgebersystems und zur Gründung der Business Keeper AG. Er engagiert sich ehrenamtlich, etwa im Deutschen Netzwerk für Wirtschaftsethik (dnwe) sowie als Leiter der Arbeitsgruppe „Hinweisgeber" von Transparency Deutschland. Er ist Referent bei Fachsymposien und Konferenzen europaweit und Autor diverser Publikationen im Kontext von Korruptionsprävention und Compliance Management.
Kontakt: redaktion@business-keeper.com