Dirk Fox

Whistleblower-Hotline

Datenschutzkonforme Gestaltung von Missstands-Meldeverfahren

Hintergrund

Mit dem Sarbanes-Oxley-Act (SOX), einer unmittelbaren Reaktion auf die Finanzskandale bei den an der New York Stock Exchange (NYSE) notierten amerikanischen Unternehmen Enron und WorldCom, verpflichtete der US-Kongress im Jahr 2002 alle an nordamerikanischen Börsen notierten Unternehmen unter anderem, ein Verfahren einzurichten, dass die anonyme Abgabe, Bearbeitung und Dokumentation von Beschwerden in Bezug auf fragliche Rechnungslegungs- oder Wirtschaftsprüfungsangelegenheiten ermöglicht.

Das dabei verwendete Verfahren ist so zu gestalten, dass ein Hinweisgeber („Whistleblower") durch die Möglichkeit zur anonymen Nutzung vor insbesondere (arbeits-) rechtlichen, aber auch vor sozialen Nachteilen geschützt wird.

Die SOX-Anforderungen gelten nicht nur für alle an einer US-Börse gelisteten Unternehmen, sondern auch für deren Tochtergesellschaften und sind daher nicht auf amerikanische Unternehmen beschränkt. Auch ist zu beobachten, dass selbst Unternehmen, die nicht in den Geltungsbereich von SOX fallen, im Rahmen ihrer Compliance-Bestrebungen so genannte „Whistleblower-Hotlines" einrichten, die die Aufdeckung und Korrektur von Fehlverhalten befördern sollen.

Spannungsfeld

Die Möglichkeit zur anonymen Abgabe von Hinweisen ist ein zentrales Element von Whistleblower-Systemen und Resultat der Beobachtung, dass sich die Meldung von Vorfällen für die Hinweisgeber in der Regel nicht auszahlt: Untersuchungen zu Folge verlieren ca. 70% anschließend ihren Arbeitsplatz.

Anonyme Meldesysteme erhöhen jedoch die Gefahr einer Persönlichkeitsverletzung für die durch einen Hinweis belasteten Mitarbeiter eines Unternehmens – und können zum Missbrauch durch Denunzianten einladen. Daher muss ein Whistleblower-System neben der Vertraulichkeit eines Hinweises und der Identität des Hinweisgebers auch die Persönlichkeit des oder der Betroffenen vor irrtümlichen, unzutreffenden oder böswilligen Beschuldigungen schützen.

In europäischen Unternehmen sind diesbezüglich insbesondere die Anforderungen der EG-Datenschutzrichtlinie zu beachten und mit den SOX-Anforderungen in Übereinstimmung zu bringen, da SOX innerhalb der EU kein unmittelbar geltendes Recht ist.

Art. 29-Gruppe

Zu diesem Spannungsfeld hat die Artikel-29-Gruppe der EU auf Betreiben der französischen Datenschutzaufsichtsbehörde CNIL, die zuvor zwei Whistleblower-Verfahren die Zustimmung versagt hatte, Anfang Februar 2006 ein Positionspapier verabschiedet [A29G06].

Kernforderung dieses Papiers ist, dass eine anonyme Whistleblower-Hotline nur für klar begrenzte Zwecke im Kontext einer nationalen Ermächtigungsgrundlage (z. B. Bankenregulierung oder Antikorruptionsgesetze) und immer nur ergänzend zu anderen vertraulichen, aber nicht anonymen Wegen zur Anzeige von diesbezüglichem Fehlverhalten angeboten werden darf.

Vor dem Hintergrund der gebotenen Erforderlichkeit und Verhältnismäßigkeit erscheit zudem eine sofortige Löschung von Vorwürfen außerhalb des vom System intendierten Zwecks geboten. Für alle anderen Daten wird eine Löschfrist von maximal zwei Monaten nach Abschluss der Ermittlungen als angemessen erachtet (vorbehaltlich anderer Erfordernisse, beispielsweise der Nutzung der Daten im Rahmen anschließender Disziplinar- oder Gerichtsverfahren).

Schließlich unterliegt die speichernde Stelle gegenüber dem Beschuldigten den gesetzlichen Auskunfts- und Informationspflichten über die über ihn gespeicherten Daten. Davon ausgenommen sind allein unbelegte oder nicht vom Zweck des Meldesystems gedeckte Vorwürfe, die unmittelbar nach Sichtung gelöscht werden, nicht aber Meldungen, die zu weiteren Untersuchungen führen, aber mit einer Einstellung der Ermittlungen enden.

Sofern damit das Risiko einer Beeinträchtigung der Aufklärung des Sachverhalts verbunden ist, kann die Benachrichtigung des Betroffenen maximal bis zum Abschluss der Ermittlungen aufgeschoben werden. Anspruch auf die Preisgabe der Identität des Hinweisgebers (sofern bekannt) hat der Beschuldigte allerdings höchstens dann, wenn jener nachweislich bösgläubig falsche Meldungen abgegeben hat.

Der Düsseldorfer Kreis hat sich in einer Stellungnahme der Bewertung und den Empfehlungen der Art.-29-Gruppe angeschlossen [DK07]. Darin wird außerdem darauf hingewiesen, dass die Einführung von Whistleblower-Hotlines der Vorabkontrolle unterliegt und daher der Zustimmung des betrieblichen Datenschutzbeauftragten vor Inbetriebnahme bedarf.

Durch ein geeignetes Sicherheitskonzept muss sichergestellt sein, dass eingehende Meldungen nur einem kleinen Kreis von Berechtigten (z. B. einem „Compliance Comittee") zum Zwecke der Bewertung und ggf. Veranlassung weiterer Ermittlungen zugänglich sind – und die festgelegten Löschregeln auch technisch verlässlich umgesetzt werden.

Literatur

[A29G06] Art. 29-Gruppe: Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen. WP 117, 00195/06/DE vom 01.02.2006

[BrKr06] Breinlinger, Astrid; Krader, Gabriela: Whistleblowing – Chancen und Risiken bei der Umsetzung von anonym nutzbaren Hinweisgebersystemen im Rahmen des Compliance-Managements von Unternehmen. RDV 2/2006

[DK07] Düsseldorfer Kreis: Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz. Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz" des Düsseldorfer Kreises, 27.04.2007.