5 Fragen an Kenan Tur über Datenschutz und Datensicherheit bei Hinweisgebersystemen

Kenan Tur, geboren 1964, wurde bei der Adam Opel AG ausgebildet, absolvierte das Studium zum Diplom-Wirtschaftsinformatiker und war bei General Motors in verantwortlicher Position im strategischen Einkauf tätig. Die Erfahrung dieser Zeit sowie sein großes Interesse an dem Thema Wirtschaftsethik inspirierten ihn zur Entwicklung eines elektronischen Hinweisgebersystems und zur Gründung der Business Keeper AG. Herr Tur engagiert sich ehrenamtlich, etwa in der Betreuung von begabten Stipendiaten in der Stiftung der Deutschen Wirtschaft (sdw), im Deutschen Netzwerk für Wirtschaftsethik (dnwe) sowie als Gruppenleiter der Arbeitsgruppe "Hinweisgeber" von Transparency Deutschland. Er ist häufig geladener Referent bei Fachsymposien und Konferenzen europaweit und Autor diverser Fachpublikationen im Kontext von Korruptionsprävention und Compliance Management.

DICO: Aus welchen Gründen setzen Unternehmen elektronische Hinweisgebersysteme ein?

Kenan Tur: Die Anzahl der Beweggründe, aufgrund derer Unternehmen ein Hinweisgebersystem implementieren, hat zweifellos zugenommen. Während sie vor sechs bis acht Jahren eher reaktiv agierten und Hinweisgebersysteme erst zum Einsatz kamen, nachdem es einen Bestechungs- oder Korruptionsvorfall gegeben hat, setzen Unternehmen sie heute immer öfter bewusst und präventiv ein. Sie signalisieren damit, dass sie für die eigenen ethisch-moralischen Verhaltensgrundsätze einstehen und straffälliges Verhalten nicht tolerieren.

Eine weitere Motivation ist die Erfüllung gesetzlicher Vorgaben. Als Teil des Compliance-Management-Systems kann ein Hinweisgebersystem dazu beitragen, Fehlverhalten intern aufzuklären und so verhindern, dass sich Mitarbeiter an die Öffentlichkeit wenden. In der Folge sinkt das Unternehmensrisiko; reputative wie monetäre Schäden können abgewendet oder reduziert werden.

Unabhängig von den unterschiedlichen Motivationen für den Einsatz eines Hinweisgebersystems hängt der Erfolg der Anwendung maßgeblich davon ab, wie gut diese in die bestehende Compliance-Struktur integriert und von den Beteiligten akzeptiert wird. Hier kommt der einführungsbegleitenden Kommunikation eine bedeutende Rolle zu.

DICO: Was sollten Unternehmen beim Betrieb von Hinweisgebersystemen aus datenschutzrechtlicher Sicht beachten?

Kenan Tur: Zunächst ist es wichtig, dass das Unternehmen das Vertrauen der potentiellen Hinweisgeber in die Anwendung und die Verarbeitung der personenbezogenen Daten gewinnt. Zu diesem Zweck müssen die Mitarbeiter umfassend über den Ablauf des Meldevorgangs informiert werden, um Ihnen die Angst vor Repressalien zu nehmen und so die Hemmschwelle zu senken, eine Meldung abzugeben.

Aus datenschutzrechtlicher Sicht ist es darüber hinaus von besonderer Bedeutung, dass die Zugriffsrechte auf die Meldungen eingeschränkt werden. Jeder Hinweis ist erst einmal eine Behauptung, die mit

personenbezogenen Daten behaftet sein kann und die es sorgsam zu prüfen gilt, um die Persönlichkeitsrechte aller Beteiligten zu wahren. Die autorisierten Mitarbeiter sollten dementsprechend sensibilisiert werden, mit den Meldungen absolut vertraulich und verantwortungsvoll umzugehen. Zudem empfiehlt es sich, die Daten ausschließlich auf Servern im europäischen Inland vorzuhalten. Und natürlich gilt es, die Löschfristen zu beachten.

Nicht zuletzt sollte die Informationsabfrage im Hinweisgebersystem für den Meldenden eindeutig und eingeschränkt sein. Dies lässt sich mit der Einrichtung von klar definierten Themenschwerpunkten gut umsetzen.

DICO: Wie können personenbezogene Daten durch ein elektronisches Hinweisgebersystem geschützt werden?

Kenan Tur: Über ein elektronisches Hinweisgebersystem können Mitarbeiter und - sofern gewünscht - externe Hinweisgeber wie z.B. Lieferanten auf interne Missstände und Risiken hinweisen. Hierbei ist es wichtig, eine autarke Anwendung anzubieten, die eine - auf Wunsch anonyme - Meldung zu vorab definierten Schwerpunkten ermöglicht.

In unserem System haben die unternehmensseitigen Hinweisbearbeiter zudem die Möglichkeit, in einen geschützten Dialog mit dem Hinweisgeber zu treten, um den Sachverhalt effizient und umfassend aufzuklären. Sollten personenbezogene Daten in einer Meldung vorhanden sein, kann ein Bearbeiter diese mit Hilfe einer Datenschutzfunktion anonymisieren. Alle mit dem System erfassten Meldungen werden unter Einhaltung strengster Datenschutz- und Datensicherheitskriterien in einem Hochsicherheitsrechenzentrum in Deutschland gespeichert. Dritte, darunter auch die Business Keeper AG selbst, haben keinen Zugriff auf die verschlüsselt abgespeicherten Meldungen. In regelmäßigen Abständen finden darüber hinaus Sicherheits- sowie Penetrationstests und -audits durch unabhängige Experten statt. Zudem wurde unser Hinweisgebersystem jüngst als erstes mit dem europäischen Datenschutzsiegel „EuroPriSe“ ausgezeichnet.

DICO: Wie ist es möglich, einerseits die Anonymität des Hinweisgebers zu schützen und andererseits eine längerfristige Dialogmöglichkeit mit dem Hinweisbearbeiter anzubieten?

Kenan Tur: Hierfür haben wir in einem mehrjährigen Entwicklungsprozess eine komplexe Technologie entwickelt, die derzeit einem Verfahrenspatent unterliegt. Sie ermöglicht den vertraulichen Dialog zwischen Hinweisgeber und -bearbeiter, der für die rasche und effiziente Hinweisbearbeitung wichtig ist. Die Anwendung unterliegt einem zertifizierten Sicherheitskonzept, das mit seinen Verschlüsselungstechniken für Datenübertragung und Datenzugriff den derzeit höchstmöglichen Standard darstellt. Damit wird die Anonymität des Hinweisgebers gewährleistet und gleichzeitig der Zugriff Dritter auf die Daten verhindert.

DICO: Wie wichtig ist die nachhaltige datenschutzkonforme Dokumentation?

Kenan Tur: Die Einhaltung von Datenschutzbestimmungen steht nicht selten im Widerspruch zur Dokumentationspflicht von Unternehmen, die sich gegenüber möglichen Nachfragen der Staatsanwaltschaft absichern möchten.

Hierfür haben wir das Case Management, das Fallbearbeitungsmodul innerhalb unseres Hinweisgebersystems, mit Hilfe von Kunden im Wirkbetrieb entwickelt. Meldungen, die in das Case Management überführt werden, können ohne die Übernahme von personenbezogenen Daten systematisch und fallspezifisch bearbeitet werden.
Des Weiteren können hier Ergebnisse und Maßnahmen festgehalten sowie Reports und Statistiken für eine übergreifende Dokumentation erstellt werden, ohne dass die datenschutzrechtlichen Belange der beteiligten Personen eingeschränkt werden. Die Möglichkeit einer nachhaltigen und datenschutzkonformen Dokumentation im Case Management kann dabei nicht nur für Meldungen aus dem Hinweisgebersystem selbst, sondern auch für Meldungen aus anderen Quellen wie Brief, Fax, Mail oder übermittelt durch einen Ombudsmann genutzt werden. Auch hier ist es vorteilhaft für Unternehmen, die Daten und somit die Dokumentation von Meldungen nicht in der eigenen IT – Infrastruktur zu bevorraten.

Lesen Sie auch die anderen Artikel zum Schwerpunktthema Compliance & Datenschutz.