

Screening von Mitarbeiterdaten: Als Maßnahme der Korruptionsprävention noch zulässig?

Von Rechtsanwältin Elke Schaefer und Wolfgang Hawreluk

Die erheblichen Anstrengungen und Erfolge der Deutschen Bahn AG zur Bekämpfung der Korruption treten durch die Daten-Affäre im Zusammenhang mit dem Abgleich der Mitarbeiterdaten mit denen von Lieferanten in den Hintergrund. Neben der zum Teil sehr pauschal geäußerten Kritik stellt sich aber berechtigterweise die Frage der Zulässigkeit von solchen Massendatenabgleichen (sog. Daten-Screening) und somit der Gefahr eines Gesetzesverstößes für die Revision bzw. Unternehmensleitung.

Der Einsatz unzulässiger Präventionsmaßnahmen schadet nicht nur der Reputation des Unternehmens sondern kann auch rechtliche Folgen wie Bußgelder, Schadensersatzforderungen der Betroffenen und unter Umständen sogar strafrechtliche Konsequenzen für die handelnden Personen nach sich ziehen.

Ein Daten-Screening ist unter Beachtung der komplexen betroffenen Rechtsgebiete, wie z.B. dem Arbeitsrecht, dem Datenschutzrecht und den Vorgaben des Grundgesetzes zulässig und als Maßnahme der Prävention und Aufklärung von Wirtschaftskriminalität auch erforderlich.

Die Zulässigkeit ist vor dem Hintergrund der jeweiligen einzelfallabhängigen Ausgangslage zu betrachten:

1. Soweit ein aus der Aussage oder (auch anonymen) Hinweisen von Dritten resultierender Korruptionsverdacht gegenüber einem oder mehreren Mitarbeiter besteht, hat das Unternehmen nicht nur das Recht, sondern die Pflicht diesen Hinweisen nachzugehen. Dazu gehört auch die Durchführung einer Corporate-Intelligence-Hintergrundrecherche über den betroffenen Mitarbeiter sowie über Lieferanten auf mögliche wirtschaftliche oder private Verflechtungen. Die gesetzliche Grundlage für die Nutzung der gespeicherten Personendaten des Mitarbeiters bildet der § 28 BDSG (siehe hierzu auch Arbeitsdokument WP 154 vom 24. Juni 2008 der Artikel-29-Datenschutzgruppe der EU), da das Unternehmen aufgrund des Anfangsverdachts ein berechtigtes Interesse nachweisen kann. Dabei ist darauf zu achten, dass für die Hintergrundrecherche ausschließlich öffentlich zugängliche Informationsquellen zur Recherche genutzt werden. Die Beschaffung bzw. Nutzung von nicht öffentlich zugänglichen Quellen (z. B. Bankkontenbewegungen, Steuererklärungen) ist nicht zulässig und gegebenenfalls sogar strafbar. Der Einsatz solcher "Beweismittel" in einem Gerichtsverfahren wird nicht zu dem gewünschten Erfolg führen.

2. Ein verdachtsunabhängiges Daten-Screening muss dem Grundsatz der Verhältnismäßigkeit wahren. Das Bundesarbeitsgericht hat zuletzt in seinem Beschluss vom 26. August 2008 (1 ABR 16/07) im Zusammenhang mit der Kontrolle von Mitarbeitern per Videoüberwachung ausdrücklich darauf verwiesen, dass solche präventiven Maßnahmen geeignet, erforderlich und unter Berücksichtigung der Gesamtumstände verhältnismäßig sein müssen, um den angestrebten Zweck zu erreichen.

Alle Mitarbeiter oder große Teile der Belegschaft eines Unternehmens im Rahmen der Korruptionsbekämpfung in einen Datenabgleich einzubeziehen, wird weder zulässig noch sinnvoll sein.

Vor dem Hintergrund des angestrebten Zieles der Prävention vor Wirtschaftskriminalität ist es zweckmäßig, Mitarbeiter aus sensiblen Unternehmensbereichen (u. a. Beschaffung, FuE) einem Datenabgleich zu unterziehen. In der Praxis sind einige Unternehmen dazu überge-

gangen sich von Mitarbeitern im Einkauf, Projektleitern und Baustellenleitern, die unmittelbar oder mittelbar in den Beschaffungsprozess involviert sind, eine Einwilligung für einen solchen Datenabgleich geben zu lassen. Andere Unternehmen gehen den Weg einer mit dem Betriebsrat getroffenen Betriebsvereinbarung. Weiterhin sollten durch unternehmensinterne Regelungen zum Umgang mit Mitarbeiterdaten Graubereiche eliminiert und Transparenz für das Unternehmen und seine Mitarbeiter geschaffen werden.

3. Sollte für ein Daten-Screening ein externes Unternehmen eingeschaltet werden, müssen Vereinbarungen zur Vertraulichkeit der Daten und der Einhaltung der datenschutzrechtlichen Bestimmungen mit dem externen Dienstleister geschlossen werden. Grundsätzlich sollten die sensiblen Daten das Unternehmen nicht verlassen und eine Speicherung auf externen Datenträgern unterbleiben.

4. Das Unternehmen hat für sich festzulegen, wie die Vernichtung der Datenträger mit den personenbezogenen Daten nach ihrer Verarbeitung und Auswertung zu erfolgen hat (hierzu bestehen einschlägige DIN-Normen über die datenschutzgerechte Vernichtung von Datenträgern).

Auch die datenschutzrechtlichen Informations- und Auskunftspflichten gegen über den Betroffenen sind vorab in die Überlegungen mit einzubeziehen.

Aus der momentanen Diskussion wird ersichtlich, dass eine große Unsicherheit über die Notwendigkeit einer Einbeziehung des Datenschutzbeauftragten und/oder Betriebsrates in solchen Fällen des Daten-Screenings besteht. Hier ist Einzelfallabhängig das Hinzuziehen zu prüfen und zu beurteilen.

Grundsätzlich sollte ein verdachtsunabhängige und auch eine verdachtsabhängige Maßnahme mit dem Datenschutzbeauftragten des Unternehmens abgestimmt werden. Gerade im Zusammenhang mit Einsichtnahme und Auswertung von Personalakten können so im Vorfall einige "Fallstricke" umgangen werden. In vielen Unternehmen stellt sich jedoch das Problem, dass eine Personalunion von Revisionsleiter – in der Regel das Durchführungsorgan eines Daten-Screenings - und dem Datenschutzbeauftragten besteht. In einem solchen Fall empfehlen wir einen im Straf- und Datenschutzrecht versierten Juristen in die Untersuchung mit einzubeziehen.

Fazit

Prinzipiell sind Daten-Screenings als effektive Mittel zur Bekämpfung von Korruption, Betrug und Untreue zu befürworten. Jedoch ist es für eine professionelle und gesetzeskonforme Vorgehensweise im Zusammenhang mit solchen Daten-Screenings notwendig, auf solche Sachverhalte spezialisierte Experten einzubeziehen. Um bußgeldbewerte Datenschutzverstöße und Schadenersatzforderungen zu vermeiden, hat ein Team aus Juristen, IT- und Datenschutzexperten die Vorgehensweise, Verarbeitung und Auswertung zu planen und zu überwachen. Somit wird gewährleistet, dass sich die Unternehmensleitung bei der Vermeidung und Aufdeckung wirtschaftskrimineller Handlungen nicht selbst strafbar macht und sich gesetzeskonform mit dem Unternehmensrisiko „Wirtschaftskriminalität“ auseinandersetzt.

Ausdruck aus www.business-integrity-management.de
Business Integrity Management GmbH ist spezialisiert auf den Schutz vor Wirtschaftskriminalität (Anti-Fraud- bzw. Anti-Korruptions-Systemen), aber ebenso bei akuten Verdachtsfällen von Betrug, Untreue, Korruption, Industriespionage oder Geheimnisverrat. Wir sind Mitglied von Integrity Europe, dem Zusammenschluss von Fraud Prevention und Investigation Spezialisten auf europäischer Ebene www.integrity-europe.eu