

Datenschutzrisiken beim Einsatz elektronischer Analyseverfahren personenbezogener Daten zur Prävention und Aufdeckung geschäftsschädigender Handlungen im Unternehmen

Autor: Rechtsanwältin Daisy Meyer-Wahl, Ressort Datenschutz und Arbeitsrecht LDM

Stellungnahme zum datenschutzkonformen Einsatz der Software REVIDATA, insbesondere unter Berücksichtigung des seit dem 01.09.2009 geltenden § 32 BDSG.

I.

Ausgangsüberlegungen/Sachverhalt

Der umfassende Abgleich von personalisierbaren Datenbeständen im Rahmen der Korruptionsbekämpfung durch den Einsatz einer Software (*Recherche und Analyseverfahren*) als Mittel der unternehmensinternen Sicherstellung von COMPLIANCE ist in den aktuellen Diskussionen zu den sog. „Datenskandalen“ in einen Zielkonflikt geraten: Berechtigte Interessen versus informationelle Selbstbestimmung.

Bei der Bekämpfung illegalen Verhaltens im Unternehmen steht das Fehlverhalten von Unternehmensangehörigen aller Hierarchiestufen einschließlich der Geschäftsleitung auf dem Prüfstand.

Ausweislich einer Studie (*KPMG 2007, S. 5*) der Wirtschaftsprüfungsgesellschaft KPMG Deutsche Treuhand Gesellschaft AG zur betrügerischen Geschäftsschädigung (*fraud*)

- handelte es sich in 89% der untersuchten Fälle um Mitbewerber des geschädigten Unternehmens,
- waren 60% der Täter Mitglieder des oberen Managements,
- waren 26% der Täter Mitglieder des mittleren Managements,
- arbeiteten die internen Täter zumeist in der Finanzabteilung einschließlich Controlling und Rechnungswesen sowie im Vertriebsbereich,
- waren auch die Vorsitzenden der Unternehmensleitungen in Teilen betroffen.

Grundsätzlich kommen als Tätergruppen bei Wirtschaftsstraftaten zu Lasten von Unternehmen, unternehmensexterne oder -interne Personen in Betracht. Zu den Externen gehören insbesondere Lieferanten, Kunden und Wettbewerber. In den Fällen, die eine Mitwirkung von Unternehmensangehörigen erfordern, bieten die Mitglieder der Geschäftsleitung, die sonstigen Führungskräfte sowie die Mitarbeiter Ermittlungsansätze und ggf. Anhaltspunkte für entsprechende Verstöße. Dass dabei auch Arbeitnehmervertreter in Erscheinung treten können, zeigen die Fälle der Volkswagen AG (vgl. z. B. Grill/Schneyink 2005) und der Siemens AG (vgl. z. B. den sog. Siemens-Skandal in Stern 24.11.2008).

Zur Erkennung geeigneter Indikatoren z. B. von Korruptionsvorgängen, auch als Bestandteil sog. Frühwarnsysteme bzw. interner Kontrollsysteme (IKS) im Rahmen des Risikomanagements, setzt die Wirtschaftspraxis automatisierte Verfahren der Informationsverarbeitung mit dem Ziel ein, rechtswidriges Verhalten beteiligter Marktpartner zu erkennen, zu vermeiden bzw. aufzuklären. Im Rahmen sog. betrieblicher „Business Intelligence“-Anwendungen sind in der Betriebswirtschaftslehre und in der Wirtschaftsinformatik automatisierte Verfahren geläufig, die das Recherche- und Analysepotential betrieblicher Datenbestände zum Teil unter Anwendung mathematisch-statistischer Verfahren auszuschöpfen suchen, um so unternehmerische Entscheidungen durch geeignete Frühwarnsysteme bzw. interne Kontrollsysteme zu unterstützen (vgl. zu solchen datenbankbasierten Anwendungen, Albers/Rüschbaum: Wirtschaftsinformatik, Stuttgart 2002, S. 108 ff.). Bei den betrieblichen Datenbeständen handelt es sich um Geschäftsdaten, die im Rahmen kaufmännischer IT-Anwendungen benötigt bzw. generiert werden. Dazu zählen auch kunden-, lieferanten- und mitarbeiterbezogene Daten.

II.

Rechtmäßigkeit elektronischer Analysen im Hinblick auf personenbezogene Daten

Nachfolgend werden die datenschutzrechtlichen Risiken elektronischer Recherche- und Analyseverfahren, wie sie zur Vorbeugung und Aufklärung illegaler Handlungen Anwendung finden, nach Maßgabe des Bundesdatenschutzgesetzes und der arbeits- und betriebsverfassungsrechtlichen Vorschriften untersucht.

§ 32 BDSG regelt den Datenschutz von Mitarbeiterdaten. Diese Vorschrift enthält in Satz 2 eine Bestimmung über den Umgang mit Mitarbeiterdaten zur Aufdeckung von Straftaten. Sofern keine Einwilligung vorliegt, dürfen zur Aufdeckung von Straftaten personenbezogene

Daten von Beschäftigten nur unter den Voraussetzungen des § 32 Abs. 1 S. 2 BDSG erhoben, verarbeitet und/oder genutzt werden. Der neue § 32 verdrängt § 28 Abs. 1 Nr. 1 BDSG als Spezialvorschrift. Die Verwendung von Daten mit indirektem oder direktem Bezug auf einzelne Beschäftigte für andere Zwecke als für das Arbeitsverhältnis kann nach § 28 Abs. 1 Nr. 2 BDSG weiterhin zulässig sein. Dies wäre z. B. der Fall bei der Überprüfung der Richtigkeit von einzelnen Buchungsvorgängen, da hier keine überwiegenden Interessen des Beschäftigten entgegenstehen. Soll konkret eine Überprüfung zur Aufdeckung einer Straftat erfolgen, ist allein § 32 BDSG einschlägig.

§ 32 BDSG Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte der Interessenvertretung der Beschäftigten bleiben unberührt.

Danach müssen dokumentierte tatsächliche Anhaltspunkte – d. h. Fakten – darauf hindeuten, dass der Beschäftigte eine beschäftigungsbezogene Straftat begangen hat. Ein „*verdachtsloser Massenabgleich*“ wäre unzulässig.

Zu prüfen ist zunächst, ob dem Einsatz der Software überhaupt personenbezogene Daten zugrunde liegen. Zum Verständnis wird angemerkt, dass sich die maschinelle Datenanalyse im Fall der Deutschen Bahn AG (*nachfolgend als „DB“ bezeichnet*) auf

Name, Adresse, Bankverbindung

bezogen und ein Abgleich von Kreditorenstammdaten mit Personalstammdaten durchgeführt worden war (*vgl. Zwischenbericht DB 12.02.2009*). Hier wurden ohne Zweifel personenbezogene Daten massenhaft abgeglichen.

Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmaren natürlichen Person (§ 3 Abs. 1 BDSG).

Sind personenbezogene Daten Gegenstand elektronischer Recherche- und Analyseverfahren, so ist deren Erhebung, Speicherung, Verarbeitung und/oder Übermittlung grundsätzlich nicht zulässig. Gleiches gilt für im Rahmen elektronischer Recherche- und Analyseverfahren bei der Verarbeitung personenbezogener Daten als Verfahrensergebnis produzierter neuer personenbezogener Daten.

Die rechtmäßige Durchführung solcher Verfahren setzt voraus, dass entweder

- die Einwilligung des Betroffenen vorliegt,
- die Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses die Datenverarbeitung rechtfertigt,
- ein berechtigtes Interesse der datenverarbeitenden Stelle oder eine gesetzliche Verpflichtung bzw. Erlaubnis vorliegt.

Maßgeblich sind insoweit die §§ 4 Abs. 1, 28 Abs. 1 S. 1, 28 Abs. 1 S. 2 BDSG.

Zulässig ist allerdings der **anonymisierte bzw. pseudonymisierte Datenabgleich** nicht personalisierter Stammdaten unterschiedlicher Personenkreise (*Mitarbeiter, Lieferanten, Kunden*) durch eine Stelle, die nicht bzw. ohne Zusatzwissen nicht in der Lage ist, den Personenbezug herzustellen. Bei einer hinreichenden Anonymisierung ist der Betroffene (z. B. *der Mitarbeiter*) nicht bestimmbar, d. h. von einem Personenbezug kann nicht ausgegangen werden.

Der Abgleich von nicht personalisierten Daten/Dateien, z. B. Kontonummern und Bankleitzahlen von Mitarbeitern einerseits und von Lieferanten andererseits mit dem Ziel der Ermittlung der Schnittmenge von Fällen, die sowohl in der mitarbeiterbezogenen als auch in der lieferantenbezogenen Datei enthalten sind, ist datenschutzrechtlich nicht zu beanstanden, wenn die **Anonymisierung** gewährleistet wird.

Voraussetzung ist insoweit, dass methodisch-technisch eine **Extraktion ausgewählter Datenfelder** aus betrieblichen Datenbeständen durchgeführt wird, also keine separate Erhebung „neuer“ Daten erfolgt.

Im vorgenannten Beispiel DB wären dies die Datenfelder „*Kontonummer*“ und „*Bankleitzahl*“ aus den Stammdatensätzen der Mitarbeiter und der Lieferanten (*Kreditoren*).

Diese Voraussetzung erfüllt die REVIDATA-Software.

Der in diesem Zusammenhang häufig geäußerte **Vorwurf des Generalverdachts**, im genannten Beispiel DB gegenüber allen Mitarbeitern und Lieferanten, geht insofern fehl, als dass die Daten ohne Ansehen der Person einem diskreten technischen Verfahren unterzogen werden, dessen Ergebnis die Selektion von Verdachtsfällen ist.

Der begründete Verdacht ist eben gerade nicht Ausgangspunkt und Impuls des Selektionsverfahrens, sondern sein erklärtes Ziel.

Ein solcher Datenabgleich mit dem Ziel der Identifikation von Verdachtsfällen setzt empirische Erkenntnisse und Plausibilitäten über solche Merkmale und deren Ausprägung (*Indikatoren*; „*Red Flags*“) voraus, die signifikant im Hinblick auf den Analysegegenstand sind.

Ist die Anzahl der in der Schnittmenge vorliegenden abgeglichenen Daten > als 0, d. h. werden tatsächlich Verdachtsfälle aufgrund von Merkmalsentsprechungen identifiziert, so kann eine Personalisierung vorgenommen werden.

Durch die Wiederherstellung des Personenbezuges und damit der Bestimmbarkeit der Betroffenen werden diese Daten (*wieder*) zu personalisierten – teilweise neuen – personenbezogenen Daten (§ 3 a S. 2 BDSG).

Erst mit Herstellen des Personenbezuges liegen personenbezogene Daten im Sinne des § 32 BDSG vor.

Spätestens dann muss die Beteiligung des Betriebsrates erfolgen (§ 80 Abs. 1 Nr. 1, Abs. 2 S. 1, § 87 Abs. 1 Nr. 6 BetrVG). Darüber hinaus hat eine Benachrichtigung bzw. Auskunft der Betroffenen zu erfolgen (§§ 4 Abs. 3, 33, 34 BDSG).

III.

Rechtskonforme Durchführung und Implementierung der Software REVIDATA

Zur Wahrung der informationellen Selbstbestimmungsrechte der Betroffenen (*Beschäftigten*) und der Mitbestimmungsrechte der Arbeitnehmervertretung sollte folgende Verfahrensweise eingehalten werden:

- Phase 1: Festlegung des Recherche- und Analyseziels
- Phase 2: Identifikation geeigneter Indikatoren
- Phase 3: Definition der abzugleichenden Datenbestände
- Phase 4: Bereitstellung eines geeigneten Softwaretools bzw. Einsatz einer geeigneten Abfragesprache
- Phase 5: Extraktion anonymisierter bzw. pseudonymisierter Daten aus den betrieblichen Datenbeständen
- Phase 6: Durchführung des Datenabgleichs
- Phase 7: Ggf. Reduktion der Schnittmenge im Ausschlussverfahren durch Anwendung weiterer Indikatoren
- Phase 8: Personalisierung der generierten Verdachtsfälle gem. § 32 BDSG

IV.

Zusammenfassung

Festzuhalten ist, dass ein automatisierter Datenabgleich auch von großen Mengen nicht personalisierter Daten mit dem Ziel der Identifikation von Verdachtsfällen grundsätzlich hinsichtlich des BDSG nicht zu beanstanden ist. Durch die Anwendung des elektronischen Analyseverfahrens wie der REVIDATA-Software werden tatsächliche Anhaltspunkte für den Verdacht des Vorliegens einer Straftat erst geschaffen. § 32 Abs. 1 S. 2 BDSG ist eine präventive und keine repressive Maßnahme (vgl. *Gesetzes-Begründung Drucks. 1613657 Deutscher Bundestag, 16. Wahlperiode*).

Voraussetzung ist, dass die Software datenschutzkonform eingesetzt wird. Folglich ist das System REVIDATA so eingerichtet, dass möglichst wenige Daten protokolliert werden. Es werden nur definierte „Trefferfälle“, die den Verdacht einer strafbaren Handlung darlegen, protokolliert und der weiteren Verarbeitung und Personalisierung zugänglich gemacht.

Das System sollte nicht heimlich eingesetzt werden, d. h. die Mitarbeiter und der Betriebsrat müssen durch den Datenschutzbeauftragten über die Funktionsweise und Umfang des Einsatzes des Systems aufgeklärt werden. Ggf. ist eine generelle vertragliche Regelung mit dem Betriebsrat über eine Betriebsvereinbarung zu treffen, unabhängig von der COMPLIANCE-Maßnahme.