Anti-Fraud-Management

Kriminalität bekämpfen mit Mitbestimmung und Datenschutz

Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen,
Matthias Wilke, Datenschutz- und Technologie-beratung (dtb), Kassel

Hier lesen Sie

- warum Betrug und Untreue nur gemeinsam mit Interessenvertretern und Datenschutzbeauftragten beizukommen ist
- welche präventiven und repressiven Methoden zur Bekämpfung von Mitarbeiterstraftaten zulässig sind
- wie eine permanente, anlasslose Rasterfahndung durch Arbeitgeber am Arbeitsplatz effektiv zu verhindern ist

© Reinhard Alff

Das Anti-Fraud-Management als Teil der Compliance in Unternehmen und Behörden bezeichnet ein System zum Vorbeugen, Entdecken und Aufarbeiten von strafbaren Handlungen wie Betrug, Korruption, Unterschlagung und Untreue. Belegschaftsvertreter haben darauf zu achten, dass diese Jagd auf Mitarbeiter etwa durch Screenings nicht aus dem Ruder läuft. Dieser Beitrag zeigt anhand eines Beispiels – Software von Wirtschaftsprüfergesellschaften soll zur Analyse großer Datenmengen im Rechnungswesen eines Unternehmens eingesetzt werden – Lösungen für ein mitbestimmungs- und datenschutzgemäßes Umsetzen von Maßnahmen zur Bekämpfung von Straftaten durch Beschäftigte.

Die Tools für Massendatenanalysen der Wirtschaftsprüfergesellschaften wie etwa Siron, IDEA, SAS oder Fraud-Scan sollen an dieser Stelle (noch) außer Betracht bleiben. Denn Tests dieser Software-Tools durch die Aufsichtsbehörden auf ihre Datenschutzkonformität und die Anforderungen an die technische Ausgestaltung in einer Orientierungshilfe stehen noch aus.

Sobald konkrete Anforderungen der Datenschützer an einen datenschutzgerechten Einsatz der Tools zur systematischen Datenanalyse vorliegen, ist es an dieser Stelle nachzulesen.

Bevor wir die Kernfrage beantworten, ob und wie der Schutz der Beschäftigtendaten bei Maßnahmen der »Fraud-Prevention« und »Fraud-Detection« und beim Einsatz derartiger Tools für Datenanalysen[1] zu gewährleisten ist, wollen wir zum besseren Verständnis noch einige zentrale Begriffe erläutern.

Begriffe bestimmen

Compliance ist das Überwachen der Einhaltung von Gesetzen und Rechtsvorschriften in den Unternehmen durch geeignete Maßnahmen und Strategien. »Compliance ist die Gesamtheit der Maßnahmen, die das rechtmäßige Verhalten eines Unternehmens, seiner Organe und Mitarbeiter im Hinblick auf alle gesetzlichen und unternehmenseigenen Gebote und Verbote gewährleisten sollen.«[2] Hier ist zu beachten, dass zu den gesetzlichen Bestimmungen auch die Datenschutzvorschriften und die Mitbestimmungsgesetze gehören. Compliance und Anti-Fraud-Management gehen nicht ohne Datenschutz und Mitbestimmung. Die Regelbefolgung unter anderem des Bundesdatenschutzgesetzes (BDSG) und des Betriebsverfassungsgesetzes (BetrVG) ist für Compliance-Aktivitäten unabdingbar.

Der englische Begriff Fraud (deutsch: Betrug, Täuschung) meint vorsätzliche, betrügerische Handlungen in Unternehmen und Behörden.[3] Als Anti-Fraud-Ma-

1 Umfassend und oftmals problematisch aus Sicht der Internen Revision GDD/DIIR (Hrsg.), Datenauswertungen und personenbezogene Datenanalyse: Beispiele für den praktischen Umgang im Revisionsumfeld, unter www.gdd.de/aktuelles/arbeitshilfen/DIIR-Datenanalyse_091209.pdf (Stand: 17.11.2013)

2 Thüsing, Arbeitnehmerdatenschutz und Compliance, 2010, Rn. 9

3 Neuber, Fraud oder betrügerische Handlungen: Was bedeutet das? Vortrag auf der 36. Dafta in Köln am 23.11.2012

nagement wird ein unternehmensweites System zur Vorbeugung, Entdeckung von und Aufdeckung »doloser« Handlungen wie Betrug, Korruption, Wirtschaftskriminalität und Untreue bezeichnet.

Fraud-Detection als ein Teil des Anti-Fraud-Managements ist das Aufdecken von Betrugsfällen durch Beschäftigte und eine Aufgabe der Compliance-Abteilung. Fraud-Prevention ist die Vorbeugung, dass es nicht zu schädigenden Handlungen durch Mitarbeiter kommt.

Der jährliche Schaden durch Mitarbeiterbetrug soll hoch sein, so zumindest das Bundeskriminalamt und Studien von Wirtschaftsprüfergesellschaften, die allerdings mit solchen Erhebungen ein eigenes wirtschaftliches Interesse verfolgen. Sie haben spezielle Analyse-Software für die systematische, automatisierte Suche nach nichtplausiblen Abweichungen unter anderem im Rechnungswesen und entsprechende Methoden – wie etwa die Benford-Analyse – entwickelt und bieten zusätzlich Audits für ein Compliance-Management-System als Dienstleistung an.

Forensische Analysen sind die Untersuchung von Dateien oder Festplatten der Mitarbeiter durch die zuständigen Stellen im Unternehmen, beispielsweise durch die IT-, Rechts- oder Revisionsabteilung.

Beschäftigtendatenschutz einhalten

Eins ist gewiss: Die Vorschriften des BDSG und der Datenschutzgesetze der Länder sind beim Einsatz von Anti-Fraud-Management-Instrumenten wie Mitarbeiter-Screening oder Whistleblowing (internes Hinweisgebersystem) insbesondere durch die Interne Revision einzuhalten.[4]

Das verdeutlichte der Fall eines großen Unternehmens, das ein automatisiertes Screening als Vollkontrolle zu Compliance-Zwecken durchführte. Dabei wurden die Kontendaten aller Beschäftigten mit den Kontennummern der Lieferanten abgeglichen, um mögliche Betrugsfälle auf Seiten der Mitarbeiter aufzudecken. Dieses anlasslose Screening war nach weit überwiegender Meinung eine rechtswidrige Rasterfahndung und somit als Datenschutzverstoß zu bewerten.[5] Dieses Beispiel zeigt anschaulich die zentralen Rechtsprobleme beim Einsatz von Compliance-Instrumenten wie dem Mitarbeiter-Screening.

Straftaten vorbeugen

Der Arbeitgeber ist grundsätzlich zu Kontrollen befugt, ob die Beschäftigten ihre Pflichten aus dem Arbeitsvertrag erfüllen.[6] Insofern sind der Einsatz von Zeiterfassung, die Kontrolle der Internetnutzung oder auch Taschenkontrollen unter Beachtung der Mitbestimmung von Arbeitnehmervertretungen, der Datenschutzgesetze und des Verhältnismäßigkeitsprinzips zulässig. Es stellt sich somit die Frage, ob und unter welchen Bedingungen Methoden der präventiven und repressiven Fraud-Bekämpfung zulässig sind.

Was ist bei Fraud-Prevention mit Hilfe von automatisierten Analysen von Beschäftigtendaten seitens des Unternehmens zu beachten? Es muss nach § 4 Abs. 1 BDSG für eine solche Datenerhebung eine rechtliche Erlaubnisvorschrift geben. Für das automatisierte Screening von Mitarbeiterdaten als Präventionsmaßnahme ist § 32 Abs.1 Satz 1 BDSG anwendbar, wenn die Maßnahme für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Allerdings muss die Maßnahme zur Datenerhebung – hier das automatisierte Screening von Geschäfts- und Rechnungswesendaten – verhältnismäßig sein, also geeignet, erforderlich und angemessen. Wenn es andere geeignetere und mildere Mittel als das automatisierte Screening gibt, ist die erfolgte Datenerhebung durch das Screening nicht erforderlich und unzulässig.

Datenschutzkonforme Datenanalysen verlangen Verdachtsmomente für Fraud oder zumindest dafür anfällige Geschäftsbereiche und zudem nur für stichprobenartige Kontrollen. Der Kreis der potenziell betroffenen Beschäftigten muss vorab eingegrenzt werden. Bei dem oben angeführten Unternehmens-Beispiel wurden Daten von Lieferanten mit Kontodaten von Beschäftigten abgeglichen, die mit dem Einkauf nichts zu tun hatten. Zudem fehlte es an Transparenz bei den Beschäftigten, die über das Screening nie aufgeklärt wurden. Es handelte sich somit um heimliche und damit das Persönlichkeitsrecht der Beschäftigten unzulässig beeinträchtigende Kontrollen.

Das stichprobenartige, automatisierte Screening muss hingegen transparent gemacht und offen durchgeführt werden. Das ist eine besonders wichtige Anforderung an ein rechtskonformes Vorgehen. Weiter ist der Zweck der Datenerhebung im Voraus eindeutig festzulegen. Sowohl bei Fraud-Prevention als auch bei -Detection müssen der betriebliche Datenschutzbeauftragte nach § 4 g Abs.1 BDSG und der Betriebsrat nach § 87 Abs. 1 Nr. 6 BetrVG so früh wie möglich und umfassend hinzugezogen werden. Das Gebot der Datensparsamkeit und Datenvermeidung gebietet es zusätzlich, stichprobenartige präventive Kontrollen nur pseudonymisiert durchzuführen und, wenn immer möglich, nur anonymisierte Daten zu nutzen.

»Datenschutzkonforme Datenanalysen verlangen Verdachtsmomente für Fraud oder zumindest dafür anfällige Geschäftsbereiche.«

Mitarbeiterüberwachung begründen

§ 32 Abs. 1 Satz 2 BDSG, der seit 2009 das betriebliche Vorgehen im Beschäftigtendatenschutz normiert, wenn ein begründeter Verdacht auf das Begehen einer Straftat im Beschäftigungsverhältnis vor-

4 Hübener, Anti-Fraud, Compliance & Datenschutz?! Eine Quadratur des Kreises? Vortrag beim Erfa-Kreis-Bremen der GDD am 22.8. 2013

5 Diller u.a., »Konten-Ausspäh-Skandal« bei der Deutschen Bahn: Wo ist das Problem? in: BB 2009, 438 ff. und Steinkühler, Kein Datenproblem bei der Deutschen Bahn? Mitnichten! in: BB 2009, 1294 f.

6 Gola/Schomerus, BDSG, 11. Auflage, § 32 Rn. 26

Beispiel für nicht rechtskonformes Vorgehen …

… bei der Aufdeckung von Straftaten oder Missbrauch im Bereich der E-Mail-Nutzung

- Bei begründetem Verdacht auf strafrechtlich relevante oder missbräuchliche beziehungsweise unerlaubte Nutzung von XXX-IT-Systemen durch einen Beschäftigten erfolgt unter Beteiligung des Betriebsrats und des Datenschutzbeauftragten eine Überprüfung durch die Geschäftsführung und/oder durch den Vorgesetzten. Die Überprüfung kann gezielte Kontrollen des dienstlichen E-Mail-Postfachs sowie anfallende Protokolldaten des Benutzens von XXX-IT-Systemen des Beschäftigten beinhalten, soweit dies nach dem Verdacht erforderlich und verhältnismäßig ist. Die Missbrauchskontrolle ist von der Geschäftsführung der XXX schriftlich oder in Textform (zum Beispiel E-Mail) anzuordnen. Auf der Basis dieser Überprüfung wird ein Bericht erstellt, der dem betroffenen Beschäftigten sowie dem Betriebsrat ausgehändigt wird. Dieser ist anschließend dazu zu hören.
- Maßnahmen, die den Missbrauch der Kommunikationsmittel verhindern oder beweisen helfen, können bei Gefahr im Verzug (begründeter Verdacht missbräuchlichen Verhaltens) unmittelbar durchgeführt werden. In diesen Fällen sind der Datenschutzbeauftragte und der Betriebsrat anschließend unverzüglich zu informieren.
- Macht das Unternehmen den Verdacht strafbarer Handlungen geltend, so wird die Angelegenheit der Staatsanwaltschaft übergeben.

liegt, kann nicht auf Fraud-Prevention angewandt werden.[7]

Es stellt sich daher die Frage, ob § 28 Abs. 1 Nr. 2 BDSG herangezogen werden kann, wenn personenbezogene Daten für die Erfüllung eigener Geschäftszwecke erhoben, verarbeitet oder genutzt werden. Gesetzliche Vorschriften verlangen vom Unternehmen, geeignete Kontrollmaßnahmen zur Vorbeugung von Korruption, Unterschlagung und Betrug, § 263 Strafgesetzbuch (StGB) durchzuführen. Hierzu gehören unter anderem § 25 c des Gesetzes über das Kreditwesen (KWG), § 130 Gesetz über Ordnungswidrigkeiten (OWiG), § 43 des Gesetzes betreffend die Gesellschaften mit beschränkter Haftung (GmbHG) und §§ 91 Abs. 2 und 93 Aktiengesetz (AktG).

Hier soll nicht der Streit darüber weitergeführt werden, ob § 28 Abs. 1 Nr. 2 oder § 28 Abs. 1 Satz 2 BDSG im Beschäftigungsverhältnis überhaupt noch anwendbar sind oder ob nur § 32 Abs. 1 Satz 1 BDSG als ausschließliche Erlaubnis für präventive Betrugsbekämpfung zutrifft. Wären beide Vorschriften anwendbar, so ist die genaue Zuordnung in der Praxis eine Einzelfallentscheidung und oftmals schwierig zu treffen.[8] Beide Vorschriften haben jedoch gemeinsam, dass stets eine Interessenabwägung und eine Verhältnismäßigkeitsprüfung verlangt werden.[9] Die Interessenabwägung und das Verhältnismäßigkeitsprinzip, das eine Datenerhebung, -verarbeitung und -nutzung erforderlich macht, gelten auch für den kirchlichen Datenschutz und für den Datenschutz im öffentlichen Bereich.

§ 28 Abs. 1 Nr. 2 verlangt ebenso wie § 32 Abs. 1 Satz 1 BDSG eine Verhältnismäßigkeitsprüfung, das heißt das schutzwürdige Interesse der Betroffenen darf an einem Ausschluss der Datenerhebung nicht überwiegen. Im Beschäftigungsverhältnis bedeutet dies, dass eine permanente Überwachung der Beschäftigten oder ein permanenter Überwachungsdruck auf die Arbeitnehmer[10] unzulässig ist, geheime oder verdeckte Kontrollen bis auf absolute Notwehrsituationen nicht möglich sind und dass das geplante Screening sich nicht auf alle Mitarbeiter des Unternehmens ohne Ausnahme als Vollkontrolle beziehen darf, sondern nur auf potenziell betrugsanfällige Geschäftsbereiche. Das Instrument einer Analyse-Software muss für den Zweck der Vorbeugung von Straftaten, Ordnungswidrigkeiten und schweren Pflichtverletzungen von Mitarbeitern geeignet, erforderlich und angemessen sein.[11]

Kontrollen einschränken

Die Betriebs- oder Dienstvereinbarung ist keine höherwertige Rechtsvorschrift im Sinne von § 1 Abs. 3 BDSG und geht damit dem BDSG nicht vor. Auch als andere Rechtsvorschrift im Sinne von § 4 Abs. 1 BDSG darf eine solche Vereinbarung nicht zu Ungunsten der Beschäftigten vom BDSG-Standard und von höherrangigem Recht abweichen und unverhältnismäßige Kontrollen der Beschäftigten vorsehen.[12]

Die Interessenvertretung ist die Hüterin des Beschäftigtendatenschutzes. Betriebsräte haben ein Überwachungsrecht nach § 80 Abs. 1 Nr. 1 BetrVG, Personalräte nach § 68 Ab. 1 Nr. 2 BPersVG und können kontrollieren, ob die Vorschriften des BDSG eingehalten werden.[13] Nach § 87 Abs. 1 Nr. 6 BetrVG (§ 75 Abs. 3 Nr. 17 BPersVG) bestimmen Betriebsräte den Einsatz von Analyse-Software wie IDEA oder AIS TaxAudit mit, die Unregelmäßigkeiten im Rechnungswesen aufdecken helfen sollen. Das bedeutet im Ergebnis, dass sowohl bei Maßnahmen der Fraud-Prevention als auch bei Maßnahmen der Aufdeckung von Betrugsfällen die Belegschaftsvertretung stets hinzuziehen ist.

Datenschutzbeauftragten einbeziehen

Bei präventiven Maßnahmen zum Vorbeugen von Betrugsfällen, die auf automatisierte Datenanalysen setzen, ist immer der Datenschutzbeauftragte hinzuziehen, der nach § 4 d Abs. 5 Satz 2 Nr. 2 BDSG

7 Zikesch/Reimer, Datenschutz und präventive Korruptionsbekämpfung – kein Zielkonflikt, in: DuD 2010, 96 ff. Auch unter http://pwcplus.pwc.de/fileserver/RepositoryItem/Fachbeitrag_Datenschutz_V04.pdf?itemId=14102192

8 Gola/Jaspers, § 32 Abs.1 BDSG – eine abschließende Regelung? in: RDV 2009, 212 ff.; neu und umfassend dazu Wolff/Brink-Riesenhuber, Datenschutzrecht in Bund und Ländern 2013, § 32 Rn. 115 ff.

9 Düwell, Verhältsnismäßigkeitsgrundsatz und Kontrolle (unveröffentlichtes Manuskript), 2012

10 Heinson/Schmidt, IT-gestützte Compliance-Systeme und Datenschutzrecht, in: CR 2010, 546 ff.

11 Zur Verhältnismäßigkeitsprüfung anhand der Rechtsprechung des BAG zur Videoüberwachung siehe Düwell, aaO.

12 Gola/Wronka, Handbuch Arbeitnehmerdatenschutz. Rechtsfragen und Handlungshilfen, 6. Auflage, Rn. 334

13 Für Personalräte entsprechend § 68 Ab. 1 Nr. 2 BPersVG

Beispiel einer Betriebsvereinbarung

Betriebsvereinbarung über die Nutzung von Analyse-Software und über forensische Analysen geschlossen zwischen …

§ 1 – Präambel

Diese Betriebsvereinbarung regelt die Einführung, den Betrieb, die Weiterentwicklung und die Änderung von Auswertungs-Software für die Interne Revision. Sie dient dem Schutz der personenbezogenen Daten der Beschäftigten und gewährleistet die Mitbestimmung des Betriebsrats, insbesondere bei der forensischen Analyse von personenbezogenen Daten der Beschäftigten. Die vorliegende Betriebsvereinbarung soll dabei Handlungssicherheit für die Verhinderung der Begehung von Straftaten beziehungsweise die Aufklärung von Straftaten schaffen und die Persönlichkeitsrechte der Beschäftigten maximal wahren.

§ 2 – Geltungsbereich

(1) Die Betriebsvereinbarung gilt für alle Beschäftigten im Sinne des § 5 Abs. 1 BetrVG einschließlich der Auszubildenden.

(2) Die Betriebsvereinbarung regelt die Einführung, den Betrieb, die Weiterentwicklung und die Änderung der Auswertungssoftware »IDEA« in der Version ____ und »TaxAudit« in der Version ___ für die Interne Revision und die damit verbundene Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten der Beschäftigten. Weiterhin werden Grundsätze für ein datenschutzkonformes Vorgehen der Revision bei der forensischen Analyse von Beschäftigtendaten festgelegt.

(3) Soweit diese Betriebsvereinbarung keine Regelung trifft, bleiben die sonstigen Rechte des Betriebsrats unberührt.

§ 3 – Zweckbestimmung

(1) Die Software »IDEA« und »TaxAudit« werden in Bezug auf Beschäftigtendaten ausschließlich für die nachfolgenden Zwecke genutzt:

- für die allgemeine prüfungsvorbereitende Datenanalyse in einem Prüfungsfeld des jährlichen Prüfungsplans der Revision,
- den Datenimport und die Umwandlung von Daten,
- und im Rahmen einer forensischen Auswertung, wenn ein durch Tatsachen konkreter, dringender und begründeter Tatverdacht vorliegt und eine anderweitige Aufklärung bis zur Einschaltung von Polizei oder Staatsanwaltschaft nicht möglich ist.

(2) Die Interne Revision nutzt die Analyse-Software »IDEA« in der Version ##.# und »TaxAudit« in der Version ##.#, um Straftaten im Beschäftigungsverhältnis wie zum Beispiel Betrug und Untreue vorzubeugen (Prävention) und aufzudecken (Repression). Der Zweck der Analyse von Daten wird vor Beginn jeder einzelnen Analyse schriftlich festgelegt.

(3) Leistungs- und Verhaltenskontrollen sind unzulässig.

(4) Die Software ist in Anlage 1 abschließend dokumentiert.

§ 4 – Stichprobenverfahren bei Nutzung von personenbezogenen Daten der Beschäftigten

(1) Für den Fall der allgemeinen prüfungsvorbereitenden Datenanalyse werden Daten der zu prüfenden Bereiche der Internen Revision bereitgestellt. Dabei werden die Beschäftigtendaten nur pseudonymisiert genutzt. Detailregelungen zur Pseudonymisierung der Daten sind in der Anlage 2 aufgeführt. Für die allgemeine prüfungsvorbereitende Datenanalyse wird ein datenschutzgerechter Ablaufplan anhand der nachfolgenden Bestimmungen von der Internen Revision und dem betrieblichen Datenschutzbeauftragten entwickelt. Es ist unzulässig, die zu nutzenden Datensätze mit dem Ziel zu verknüpfen, personenbezogene Daten einzelnen Beschäftigten zuordnen zu können.

(2) Die Interne Revision setzt im Rahmen der allgemeinen prüfungsvorbereitenden Datenanalyse die Stichprobenanalyse in zwei Varianten ein.

Die erste Variante der Stichprobe ist die Zufallsstichprobe. Für diese wird mit Hilfe der Analyse-Software der Stichprobenumfang definiert und aus der Gesamtmenge die auszuwählenden Datensätze der Zufallsstichprobe ermittelt. Nur diese Datensätze werden einer genaueren Analyse unterzogen.

Die zweite Variante der Stichprobe ist die bewusste Stichprobe. Für diese wählt der Prüfer anhand von vorher definierten oder bei Durchsicht der Daten erkannten Auffälligkeiten der Daten die Datensätze der Stichprobe aus.

§ 5 – Auffälligkeiten bei Datenanalysen

(1) Nichtauffällige Ergebnisse der Datenanalysen werden unverzüglich gelöscht. Wenn im Rahmen von Datenanalysen Auffälligkeiten entdeckt werden, werden die in der Internen Revision pseudonymisiert vorhandenen Daten an die interne Stelle gegeben, die gegebenenfalls zur Klärung beitragen kann. Die Stelle kann zum Beispiel die Personalabteilung, das Rechnungswesen oder die IT-Abteilung sein. Die Beschäftigten der internen Stellen werden zur Verschwiegenheit verpflichtet.

- Wenn eine schlüssige Erklärung für die Auffälligkeit besteht, erhält die Interne Revision diese ohne Nennung von Personennamen.
- Sollten die Auffälligkeiten nicht erklärt werden können, so dass ein durch zu dokumentierende tatsächliche Anhaltspunkte begründeter Tatverdacht gegen eine bestimmte Person oder einen bestimmten Personenkreis vorliegt, werden die Geschäftsführung und der Betriebsrat zeitgleich und unverzüglich informiert. Die weitere Vorgehensweise ist wie im Fall einer forensischen Auswertung eines durch Tatsachen begründeten konkreten Tatverdachts zu behandeln.

§ 6 – Einsatz der Analyse-Software zur forensischen Analyse

(1) Der Einsatz der Analyse-Software mit personenbezogenen Daten der Beschäftigten zur forensischen Analyse ist nur erlaubt, wenn durch Tatsachen beziehungsweise zu dokumentierende Anhaltspunkte ein begründeter, konkreter und dringender Tatverdacht vorliegt und eine Verarbeitung und Nutzung dieser personenbezogenen Daten der Beschäftigten erforderlich ist. Auch ein weiterer Einsatz der Analyse-Software ohne die Verarbeitung und Nutzung von Beschäftigtendaten ist möglich, ebenso wie der Einsatz anderer Revisionsmethoden ohne DV-Unterstützung. Für die forensische Analyse wird ein datenschutzgerechter Ablaufplan von der Revision

und dem Datenschutzbeauftragten anhand der nachfolgenden Bestimmungen erstellt. Dieser wird dem Betriebsrat auf Verlangen vorgelegt:

- Wenn die Analyse-Software (IDEA, TaxAudit) zur forensischen Analyse eingesetzt und personenbezogene Daten der Betroffenen erhoben, verarbeitet und genutzt werden sollen, weil ein durch Tatsachen begründeter konkreter Verdacht vorliegt und eine anderweitige Aufklärung bis zur Einschaltung von Polizei oder Staatsanwaltschaft nicht möglich ist, ist vorher die Zustimmung der Geschäftsführung und des Betriebsrats nach erfolgter und dokumentierter Zulässigkeits- und Verhältnismäßigkeitsprüfung einzuholen. Bei der Verhältnismäßigkeitsprüfung ist der betriebliche Datenschutzbeauftragte hinzuziehen. Die den Verdacht begründenden Tatsachen sind von der Internen Revision vollständig und abschließend zu benennen und dem Datenschutzbeauftragten und dem Betriebsrat mitzuteilen.
- Bei forensischen Analysen werden die Daten hinsichtlich der Beweissicherung oder Entlastung des/der betroffenen Beschäftigten analysiert. Zu wahren ist dabei der Grundsatz der Datenvermeidung und Datensparsamkeit.
- Nach Abschluss der Untersuchungen sind die Ergebnisse zu protokollieren und ein Bericht zu erstellen. Die Geschäftsführung erhält nach Abschluss der Untersuchungen den Revisionsbericht (Dokumentation) über die mit Hilfe der Revisions-Software durchgeführten Untersuchungen gegen konkret verdächtigte Personen und leitet diesen unmittelbar an den Betriebsrat weiter.
- Nach erfolgter Untersuchung ist der betroffene Beschäftigte über die Datennutzung unverzüglich beziehungsweise so früh als möglich zu unterrichten. Sollte der Verdacht auf Begehung einer Straftat gegenstandlos werden, sind sämtliche Unterlagen und Daten aus den Analyseschritten (wie E-Mails, Tabellen, Ausdrucke) unverzüglich zu vernichten. Die gefundenen Ergebnisse (Zufallsfunde) dürfen nicht für andere Zwecke verwendet werden. Arbeitsrechtliche Maßnahmen sind unzulässig. Etwas anderes gilt nur, wenn bei der Auswertung anderweitige Straftaten oder schwerwiegende Verstöße gegen Gesetze und die geltenden Richtlinien im Unternehmen entdeckt werden.
- Ist der Verdacht nicht ausgeräumt, ist der Ergebnisbericht dem betroffenen Beschäftigten unverzüglich auszuhändigen. Der Betroffene ist anzuhören. Auf Wunsch des Betroffenen ist ein Mitglied des Betriebsrats zur Anhörung hinzuzuziehen.
- Alle Maßnahmen und Informationen/Daten sind von allen Beteiligten vertraulich zu handhaben.

(2) Der betriebliche Datenschutzbeauftragte prüft jährlich die Einhaltung dieser Betriebsvereinbarung und informiert die Geschäftsführung und den Betriebsrat über die Ergebnisse seiner Prüfung. Damit dies möglich ist, verpflichtet sich die Revision, die Ergebnisse der Analysen und durchgeführte Arbeiten mit der Software, bei denen personenbezogene, pseudonymisierte Daten genutzt wurden, in einem jährlichen Revisionsbericht zu dokumentieren, der dem Betriebsrat mit dem Bericht des betrieblichen Datenschutzbeauftragten zur Kenntnis gegeben wird.

(3) Werden Informationen beispielsweise aus den Analysen unter Verletzung der Bestimmungen dieser Betriebsvereinbarung und des Persönlichkeitsrechts der Beschäftigten gewonnen, weiterverarbeitet und genutzt, dürfen diese nicht zur Begründung personeller oder arbeitsrechtlicher Maßnahmen wie zum Beispiel Kündigung genutzt werden. Solche Maßnahmen sind unwirksam. Die unrechtmäßig gewonnenen Informationen und Daten unterliegen einem Beweisverwertungsverbot. Dies gilt auch für Zufallsfunde und Ermittlungsergebnisse, die unter Verstoß gegen diese Betriebsvereinbarung zustande gekommen sind. Sie dürfen durch das XXX nicht zum Gegenstand einer Sanktion oder eines gerichtlichen Verfahrens gemacht werden.

(4) Bei Verstößen gegen Bestimmungen der Betriebsvereinbarung muss mit arbeitsrechtlichen Konsequenzen gerechnet werden.

(5) Die Interne Revision informiert den Betriebsrat bei Vorliegen eines Updates der Analyse-Software und stellt die Herstellerdokumentation zu den Neuerungen dem Betriebsrat zeitnah zur Verfügung. Die regelmäßigen Updates zur Fehlerbehebung, durch die die Funktionalitäten der Software unverändert bleiben, können ohne vorherige Zustimmung des Betriebsrats eingesetzt werden. Wenn ein Update neue Funktionen zur Verfügung stellt, ist die vorherige Zustimmung des Betriebsrats einzuholen.

Es folgen die üblichen Schlussbestimmungen …

eine Vorabkontrolle durchzuführen hat. Bei geplanten Screenings von Daten im Rechnungswesen handelt es sich nicht nur – aber auch – um personenbezogene Daten der Beschäftigten, die zum Beispiel diese Geschäftsvorfälle bearbeiten, und somit um eine Bewertung der Person und des Verhaltens dieser Mitarbeiter.

Die Pflicht, den Datenschutzbeauftragten zu beteiligen, gilt ebenso für die Aufdeckung und Aufklärung von Straftaten, die gegen das Unternehmen gerichtet sind. Hat der Datenschützer Zweifel an einem datenschutzkonformen Vorgehen oder bereits an der Zulässigkeit von präventiven oder repressiven Maßnahmen der Fraud-Bekämpfung, hat er die Aufsichtsbehörde für den Datenschutz einzuschalten.

Straftaten aufdecken

Die neue Vorschrift in § 32 Abs. 1 Satz 2, die sich an § 100 Abs. 3 Satz 1 Telekommunikationsgesetz (TKG) orientiert, ist sehr bestimmt und setzt hohe Anforderungen an ein datenschutzkonformes Vorgehen beim Aufdecken von Straftaten im Beschäftigungsverhältnis. Nach wie vor haben Arbeitgeber Schwierigkeiten mit den Anforderungen an ein verhältnismäßiges Vorgehen und vereinfachen die rechtlichen Anforderungen oftmals in unzulässiger Weise. Wiederholt wird das offenkundig, wenn es um die Kontrolle der Nutzung von E-Mail im Unternehmen geht.

Das Beispiel auf Seite 6 aus einer Betriebsvereinbarung zur Nutzung von E-Mail, vorgelegt von der Arbeitgeberseite, zeigt ein mangelndes Bewusstsein davon, was der § 32 Abs.1 Satz 2 BDSG voraussetzt und führt zudem die Beteiligung des Betriebsrats und des Datenschutzbeauftragten nur ungenau aus. Die »Gefahr im Verzug« führt dazu, dass die Interessen-

vertretung nach vollzogenen Maßnahmen anschließend nur ein nachträgliches Anhörungsrecht hat. Rechte der betroffenen Beschäftigten sind nicht geregelt. Das arbeitgeberseitige Vorgehen insgesamt ist nicht transparent. Was ein begründeter Verdacht sein soll, wird nicht ausgeführt. Die erforderliche Verhältnismäßigkeitsprüfung wird nur vorausgesetzt aber nicht konkretisiert. Die Anhaltspunkte für eine Straftat werden nicht vorab dokumentiert.[14]

§ 32 Abs. 1 Satz 2 BDSG als bestimmter Erlaubnistatbestand bezieht sich auf Straftaten im Beschäftigungsverhältnis und verlangt einen sehr konkreten, begründeten und zu dokumentierenden Anfangsverdacht, damit die anschließende Datenerhebung, -nutzung und -verarbeitung der Daten der betroffenen Beschäftigten rechtmäßig ist.

Hinzu kommt, dass die Vorschrift immer eine Interessenabwägung im Sinne einer Verhältnismäßigkeitsprüfung verlangt. Ist die Datenerhebung erforderlich oder ist im Sinne von Datensparsamkeit und Datenvermeidung darauf zu verzichten? Nur die erforderlichen personenbezogenen Daten dürfen erhoben, genutzt und verarbeitet werden.

Grundsätzlich ist immer das Erheben der Daten pseudonymisiert durchzuführen und erst wenn sich ein konkreter durch Tatsachen begründeter Verdachtsfall ergibt, dürfen die Daten personalisiert werden. Tatsachen sind Indizien für einen Straftatbestand.[15]

Bei der Verhältnismäßigkeitsprüfung sind weiterhin die Schwere der Straftat und die Intensität des Verdachts zu berücksichtigen.[16]

Auf den Seiten 7 und 8 wird eine Betriebsvereinbarung dokumentiert, die sich zum Ziel gesetzt hat, ein datenschutzkonformes Vorgehen beim Einsatz von selektiven stichprobenartigen automatisierten Datenanalysen und forensischen Analysen zur Aufdeckung von Straftaten zu vereinbaren.

Anti-Fraud-Maßnahmen regeln

Die Betriebsvereinbarung ab Seite 7 regelt den offenen automatisierten Einsatz von Wirtschaftsprüfer-Software, die zum Zweck der Prävention und Aufdeckung von Fraud im Bereich des Rechnungswesens durch die Interne Revision eingesetzt werden soll. Diese Vereinbarung ist ein betrieblicher Kompromiss. Zweck der Betriebsvereinbarung ist die abschließende Festlegung eines datenschutzkonformen und legalen Vorgehens für die Interne Revision.

Im Vorfeld wurden als mildere Mittel organisatorische Maßnahmen eines internen Kontrollsystems und Risikomanagements umgesetzt, die vor allem auf nichttechnische und organisatorische Kontrollmaßnahmen abzielen und unter anderem ein Sicherheitssystem, die Festlegung von Verantwortlichkeiten, Mitarbeiterinformation und -schulung, Nutzung eines Vier-Augen-Prinzip, Sicherheitsrichtlinien und manuelle Prüfhandlungen – wie die Prüfung von Unterlagen – vorsehen.

Anlass für die Verhandlung der Betriebsvereinbarung war ein größerer Betrugsfall, der ein fehlendes Kontrollsystem beziehungsweise Risikomanagement im Rechnungswesen des Unternehmens verdeutlichte und dieses als Risikobereich offenbarte. Vorab ist in diesem Beispiel eine detaillierte Risikoanalyse durchgeführt worden, was bei allen Maßnahmen des Anti-Fraud-Managements unabdingbar ist.

Die abgeschlossene Betriebsvereinbarung sieht stichprobenartige Kontrollen und keine automatisierten Massendatenanalysen mit Geschäfts- und Rechnungswesendaten vor, trennt transparent zwischen präventiven und repressiven Maßnahmen und vermeidet eine lückenlose automatisierte Kontrolle, in dem eine Überprüfung und Klärung vor Ort ohne Einschaltung der Internen Revision durch andere zuständige oder betroffene Abteilungen vorgesehen wird. In diesem Fall geht es vielmehr um das Etablieren eines gestuften, langsam eskalierenden Kontrollverfahrens.[17]

Gleichzeitig sollte aus Sicht des Betriebsrats die Arbeit der Revision nicht

© Wolfgang Zwanzger, Fotolia

Für ein rechtmäßiges Screening der Mitarbeiter sind konkrete Verdachtsmomente nötig.

14 Dagegen ist das konkrete Verfahren bei Verdacht auf Begehung einer Straftat unter dem Begriff der doppelte Sachverhaltsprüfung vorbildlich geregelt in §§ 18, 19 der KBV Beschäftigtendatenschutz im DB- Konzern, www.evg-online.org/Arbeitswelt/Mitbestimmung/Betriebsverfassung/.Aktuelles/13_04_10_KBV_BDS/ (Stand: 17.11.2013)

15 Gola/Schomerus, aaO. und insgesamt Gola/Wronka, aaO., Rn. 1199 ff.

16 Thüsing, aaO., Rn. 146 ff.

17 Für Kontrolle von E-Mails siehe das Eskalationsmodell des ULD Schleswig-Holstein, www.datenschutzzentrum.de/internet/private-und-dienstliche-internetnutzung.pdf (Stand: 17.11.2013)

unnötig erschwert werden, die den Grundsatz der Verhältnismäßigkeit bei allen Prüfhandlungen zu beachten hat.

Vorgehen festlegen

Das Kontrollverfahren lässt sich zusammenfassend wie folgt beschreiben: Zunächst erfolgt die Festlegung eines Prüfungsplans mit stichprobenartigen Kontrollen durch die Revision. Dann werden Daten, Geschäftsvorfälle und Belege auf Auffälligkeiten analysiert, wobei ein Personenbezug der Daten infolge von Pseudonymisierung nicht gegeben ist. Für diese Datenanalyse kann die Software im Sinne der abschließend festgelegten Zweckbestimmung genutzt werden. Dabei können sich Auffälligkeiten und Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben, für die es keine augenfälligen Erklärungen gibt.

Diese Indizien oder Auffälligkeiten werden dokumentiert und führen zur Einschaltung einer internen Stelle wie der IT-Abteilung oder der Personalabteilung, die zunächst abgeschottet von der Revision nach Erklärungen für das auffällige Abweichen von der Norm sucht.

Kann keine plausible Erklärung gefunden werden, kommt es zur speziellen personalisierten Datenanalyse durch die Revision und damit zur De-Pseudonymisierung der Daten, wobei vorher der Datenschutzbeauftragte einbezogen wird und die Belegschaftsvertretung zustimmen muss. Die explizite Zustimmung ist zur Absicherung des Arbeitgebers unerlässlich, da ansonsten arbeitsrechtliche Maßnahmen bei einem Datenschutzverstoß gemäß § 138 Abs. 1 BGB nichtig werden können.[18]

Erst bei einem hinreichend begründeten Anfangsverdacht mit entsprechenden Indizien gegen einen oder mehrere konkret benannte Beschäftigte und einer dokumentierten Verhältnismäßigkeitsprüfung werden entsprechende Maßnahmen eingeleitet, um den Verdacht einer Begehung von Straftaten im Beschäftigungsverhältnis zu überprüfen. Lässt der Verdacht sich dann von der Revision nicht hinlänglich aufklären, wird der betroffene Beschäftigte benachrichtigt.

Weitere konkrete Maßnahmen der Aufarbeitung von Betrugsfällen etwa beim Auswerten der Protokolldaten oder der dienstlichen E-Mails werden in dieser Betriebsvereinbarung nicht geregelt, da deren Schwerpunkt auf die Fraud-Prevention, die Aufdeckung von Betrugshandlungen und den Einsatz der speziellen Tools für die Revision gelegt worden ist.

»Compliance, Anti-Fraud-Management, Mitbestimmung und Datenschutz sind auch bei der Prävention und Aufdeckung von Betrugsfällen ganzheitlich zu sehen und dürfen nicht gegeneinander ausgespielt werden.«

Ein weiteres Ziel des Betriebsrats war es, Datenschutzprinzipien wie Zulässigkeit, Zweckbindung, Transparenz, Datensparsamkeit und Verhältnismäßigkeitsprinzip/Erforderlichkeit so weit wie möglich zu konkretisieren und alle Kontrollinstanzen des Beschäftigtendatenschutzes in die Prozessbeschreibung von Fraud-Prevention und -Detection zu integrieren. Leistungs- und Verhaltenskontrollen werden ausgeschlossen. Über die Betriebsvereinbarung wird auf verschiedene Weise im Unternehmen informiert und somit für die Beschäftigten die datenschutzrechtliche Transparenz hergestellt.

Fazit

Die präventive und repressive Bekämpfung von Betrug und Untreue ist nur mit Datenschutz und Mitbestimmung möglich. Compliance, Anti-Fraud-Management, Mitbestimmung und Datenschutz sind auch bei der Prävention und Aufdeckung von Betrugsfällen im Unternehmen ganzheitlich zu sehen und dürfen nicht gegeneinander ausgespielt werden.

Die vorliegende Beispiel-Betriebsvereinbarung (Seite 7 und 8) zeigt einen gemeinsamen Weg von Arbeitgeber, Revision und Betriebsrat, möglichst in allen Prozessschritten von Compliance und Anti-Fraud-Management größtmögliche Rechtskonformität sicherzustellen, das heißt die verabredeten Maßnahmen erfolgen offen, differenziert und auf gesetzlicher Grundlage.[19]

Die Betriebsparteien haben verabredet, die Betriebsvereinbarung anhand der Erfahrungen mit der Analyse-Software und tatsächlicher Auffälligkeiten nach zwei Jahren zu überprüfen und erforderliche Verbesserungen des Beschäftigtendatenschutzes vorzunehmen. Das Beispiel zeigt zudem, dass der Betriebsrat als Datenschützer im Unternehmen tätig werden kann und die Arbeit der Internen Revision mit speziellen Tools zur Massendatenanalyse unbedingt überprüfen und mitgestalten sollte. Der flächendeckende Einsatz etwa der Unternehmens-Software SAP ERP[20] führt zu Big Data[21] auch in der Privatwirtschaft und zum verstärkten Interesse an Tools für Data Mining.[22] Hier ist die Interessenvertretung als Hüter des Beschäftigtendatenschutzes gefordert.

Autoren

Dr. Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen
» eberhard.kiesche@t-online.de
» www.aob-bremen.de

Matthias Wilke, Datenschutz- und Technologieberatung (dtb), Kassel
» info@dtb-kassel.de
» www.dtb-kassel.de

cua-web.de

SERVICE

Arbeitshilfen » Mustervereinbarung ✔

18 Siehe BAG vom 15.11.2012, Az.: 6 AZR 339/11, in: DB 2013, 584

19 Brink, Anti-Fraud-Management. Compliance vs. Mitarbeiter-Datenschutz, Vortrag am 23.11.2012 auf der Dafta in Köln

20 Wilke (Hrsg.), SAP kompakt für den Betriebsrat, 2014

21 Höller, Big-Data-Analysen, in: CuA 11/2013, 4 ff.

22 Siehe dazu auch Hirsch, Verbrecherjagd mit Data Mining, in: CuA 3/2010, 27 ff.