

# Handlungsempfehlungen beim Datenabgleich zur Auf- deckung wirtschaftskrimi- neller Handlungen durch die Interne Revision

Volker Hampel, DIIR, in Zusammenarbeit mit den Arbeitskreisen „Abwehr wirtschaftskrimineller Handlungen in Unternehmen“ und „Interne Revision im Mittelstand“ des DIIR

*Nach vorliegenden Studien gehen deutsche Unternehmen mit deutlicher Mehrheit davon aus, dass die Anzahl wirtschaftskrimineller Handlungen in Unternehmen künftig zunehmen oder zumindest auf dem derzeitigen Niveau stagnieren wird. Die Unternehmensleitungen sind gefordert, geeignete Kontrollsysteme vorzuhalten, die eine ordnungsgemäße Unternehmensführung – einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen – sicherstellen. Die Interne Revision gehört hier eindeutig zu den Kernelementen des Kontrollsystems und bedient sich – wie andere Prüfer – bereits seit vielen Jahren auch der Analyse von Datenbeständen. Wesentliche Argumente sind die deutlich höhere Effizienz bei analytischen Prüfungen und die Notwendigkeit, wirtschaftskriminelle Handlungen möglichst systematisch und frühzeitig zu erkennen. Grenzen bei der Analyse von Datenbeständen liegen dabei in der Beachtung regulatorischer Vorschriften. Bei personenbezogenen Daten ist die Berücksichtigung des Bundesdatenschutzgesetzes zwingend erforderlich.*

## 1. Wirtschaftskriminalität in deutschen Unternehmen

Nach vorliegenden Polizeilichen Kriminalstatistiken<sup>1</sup> bewegte sich die Zahl in Deutschland registrierter wirtschaftskrimineller Handlungen in den letzten 5 Jahren (Betrachtungszeitraum 2003 bis 2007) jeweils zwischen ca. 81.000 und ca. 95.000 p. a. Die hierbei registrierten Schäden beliefen sich laut Bundeskriminalamt (BKA) auf ca. 4,12 Milliarden Euro (2007). Die zur Bewältigung dieser Straftaten erforderlichen Kosten werden im gleichen Zeitraum auf ca. 1,75 Milliarden Euro taxiert<sup>2</sup>.

Nach Einschätzung des BKA dürften die genannten Werte nur einen Ausschnitt des tatsächlichen Ausmaßes wiedergeben (u. a. wegen restriktiven Anzeigeverhaltens aus Furcht vor Imageverlusten). Eine Studie von PricewaterhouseCoopers (PWC) sieht in deutschen Unternehmen im internationalen Vergleich Nachholbedarf bei der Kriminalitätsbekämpfung<sup>3</sup>.

Nach einer aktuellen Studie der Euler Hermes Kreditversiche-  
rung<sup>4</sup> gehen deutsche Unternehmen mit überwiegender Mehr-

heit (91 %) davon aus, dass die Anzahl wirtschaftskrimineller Handlungen zukünftig mindestens stagnieren (46 %) bzw. zunehmen wird (45 %). Meist wurden laut Euler Hermes wirtschaftskriminelle Handlungen bei befragten Unternehmen von Fachkräften und „sonstigen Angestellten“ (71 %) begangen<sup>5</sup>. Aufgedeckt wurden die Handlungen am häufigsten durch „das Interne Kontrollsystem bzw. die Interne Revision“ (47 % der Fälle)<sup>6</sup>.

Zusammenfassend kann also festgehalten werden, dass präventive Maßnahmen als Teil einer angemessenen Unternehmens-Organisation und -kontrolle (auch im Rahmen gesetzlicher Vorschriften wie insbesondere §91 (2) Aktiengesetz [AktG]) angebracht sind.

## 2. Regulatorischer Hintergrund und Internes Kontrollsystem

§91 (2) AktG fordert die Einrichtung eines Überwachungssystems, um „... den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig zu erkennen.“ Im Schrifttum wird von einer Ausstrahlungswirkung des §91 (2) AktG auch auf andere Rechtsformen – insbesondere Kapitalgesellschaften – ausgegangen. Gemäß §93 (2) AktG sind Vorstandsmitglieder bei schuldhafter Pflichtverletzung (also bspw. Unterlassen der Einrichtung eines Überwachungssystems) gesamtschuldnerisch schadensersatzpflichtig.

Dem Internen Kontrollsystem (IKS) kommt laut IDW PS 261<sup>7</sup> unter anderem die Zielsetzung „... Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäfts-

tätigkeit (hierzu gehört auch der Schutz des Vermögens, einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen), ...“ zu. Die Funktionsfähigkeit des IKS wird wiederum vor allem von der Internen Revision durch prozessunabhängige Überwachungsmaßnahmen geprüft<sup>8</sup>.

Über das Gesetz zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz – BilMoG)<sup>9</sup> werden insbesondere in Aktiengesetz (AktG) und Handelsgesetzbuch (HGB) diverse An-

1 Vgl. BKA, (o. Datum), S. 5 ff.

2 Vgl. PwC (2007), S. 3.

3 Vgl. PwC (2007), S. 4.

4 Vgl. Euler Hermes (2008), S. 6.

5 Vgl. Euler Hermes (2008), S. 11.

6 Vgl. Euler Hermes (2008), S. 17.

7 Vgl. IDW (2006), S. 1437.

8 Vgl. Schartmann/Lindner, in: Lück (2006), S. 38 f.

9 Vgl. Deutscher Bundestag (2008). Der Gesetzentwurf wurde vom Deutschen Bundestag am 26. 3. 2009 und vom Deutschen Bundesrat am 3. 4. 2009 verabschiedet.

passungen zur Überwachung der Funktionsfähigkeit und Wirksamkeit des IKS, des internen Risikomanagementsystems und des „internen Revisionssystems“ vorgenommen<sup>10</sup>. Branchenspezifische Regelungen für die Einrichtung interner Kontrollverfahren und -systeme finden sich beispielsweise im Kreditwesengesetz<sup>11</sup>.

Als internationales Beispiel ist ergänzend die U. S. Securities and Exchange Commission (SEC) zu nennen. Auch sie zählt das „safeguarding of assets“ in der Kommentierung zum US-amerikanischen Sarbanes-Oxley Act von 2002 (section 404) zu den Elementen des IKS<sup>12</sup>. Explizit werden Kontrollen zur Vermeidung, Identifikation und Aufdeckung von Betrug gefordert. Hierzu sind geeignete Prozeduren zur Überprüfung der Angemessenheit und der Funktionsfähigkeit des IKS zu schaffen. Dabei ist die reine Befragung oder Erhebung nicht hinreichend – vielmehr ist durch angemessene Dokumentation und geeignete Testprozeduren der Nachweis der Funktionsfähigkeit des IKS zu erbringen. In Ergänzung fordert der Foreign Corrupt Practices Act von 1977 (FCPA) interne Kontrollen zur Identifikation sogenannter „Red Flags“ (Hinweise auf betrügerisches Verhalten)<sup>13</sup>.

### 3. Fraud Prevention and Detection mit IT-gestützten Prüfungstechniken

Zur Erfüllung der Forderung nach Fraud Prävention sind unterschiedliche Ansätze denkbar. Neben der strukturierten Durchführung von Prozesskontrollen in risikobehafteten Bereichen ist auch die Analyse von Datenbeständen wichtig<sup>14</sup>. Ziel ist es, über reine Stichprobenprüfungen hinaus systematisch und strukturiert nach Anhaltspunkten/Frühwarnindikatoren (also „Red Flags“) für wirtschaftskriminelle Handlungen zu suchen – hierzu müssen keine konkreten Verdachtsmomente vorliegen.

Eine angemessene Effizienz von Prüfungshandlungen wird bei der Analyse von Datenbeständen – nicht nur im Zusammenhang mit Fraud-Untersuchungen – erst durch den Einsatz IT-gestützter Prüfungstechniken ermöglicht. So sieht das IDW (PS 330<sup>15</sup>) in der Verwendung IT-gestützter Prüfungstechniken einen Weg, die Wirksamkeit und Wirtschaftlichkeit von Prüfungen wesentlich zu erhöhen. Voraussetzung sind hier laut IDW das Vorliegen von elektronischen Belegen oder Prüfungen im Zusammenhang mit einer sehr großen Anzahl von Geschäftsvorfällen.

IT-gestützte Analysen gehören daher bereits seit vielen Jahren zum etablierten Tagesgeschäft von Prüfern (Wirtschaftsprüfer, Steuerprüfer, Interne Revisoren etc.). Oft haben die oben genannten strukturierten Analysen im Zusammenhang mit Fraud Detection eher einen Vollprüfungs- als einen Stichproben-Charakter (sie zielen auf die Untersuchung einer mög-

lichst umfassenden Grundmenge von Daten statt nur einer repräsentativen Stichprobe ab). Dort sind IT-gestützte Prüfungstechniken zur Datenanalyse – auch aufgrund der Menge gleich strukturierter Daten und der wesentlich höheren Geschwindigkeit des automatisierten Datenvergleichs – einem physischen Belegvergleich weit überlegen.

Daher kommen seit vielen Jahren diverse IT-gestützte Tools (wie z. B. IDEA, ACL, SAS, SiRON, FRAUD-SCAN, AIS, Analyst's Notebook, Qlikview etc. mit teilweise variierenden Schwerpunkten) zum Einsatz, die benutzerdefinierte Abfragen erlauben oder in denen bereits vordefinierte Standardmodule verfügbar sind (wie bspw. statistische Analysen, Korrelationen und Zeitreihen bis hin zur Visualisierung von sozialen Netzwerken aus Datenbeständen im Zusammenhang mit Geldwäsche-Untersuchungen). Diverse Tools sehen als Grundfunktion ebenfalls den Abgleich von Datenbeständen vor und werden in Deutschland auch von öffentlichen Institutionen (bspw. Finanzverwaltungen) genutzt.

Der Abgleich strukturierter Datenbestände erlaubt beispielsweise die Erkennung von Doppel-, Mehrfachrechnungen oder gleicher Kontodaten in unterschiedlichen Dateien. Ebenso ist die Häufung von Merkmalen innerhalb bestimmter definierter Kategorien (bspw. gehäuftes Auftreten von Rechnungsbeträgen knapp unterhalb einer definierten Freigabegrenze) systematisch analysierbar. Derartige Analysemöglichkeiten sind für die Identifikation und Aufdeckung von Betrugsfällen in Unternehmen essentiell.

### 4. Grenzen der Analyse von Datenbeständen

Grenzen bei der Analyse von Datenbeständen liegen unter anderem in der Verfügbarkeit und Nutzbarkeit der benötigten Daten, aber auch in der Beachtung regulatorischer Vorschriften. Bei der Analyse personenbezogener Daten ist die Berücksichtigung der bestehenden Datenschutzvorschriften des Bundesdatenschutzgesetzes<sup>16</sup> zwingend erforderlich.

So ist der Datenschutzbeauftragte gem. § 4g (1) BDSG über Vorhaben zur automatisierten Analyse personenbezogener Daten rechtzeitig zu unterrichten bzw. sind die bei der Analyse personenbezogener Daten tätigen Personen mit den geltenden Vorschriften des BDSG – bspw. durch den Datenschutzbeauftragten – vertraut zu machen. Hierzu gehört auch eine Übersicht über die auf die Datenbestände zu-

10 Vgl. Deutscher Bundestag (2008): §§ 107 und 171 AktG, §§ 289 (5), 324 HGB.

11 Vgl. Bundesministerium der Justiz (2009a): §§ 25a und 25c KWG.

12 Vgl. SEC (2003): Sec. II.B.3.d., abrufbar unter: <http://www.sec.gov>.

13 Vgl. U. S. Department of Justice (1998), 15 U.S.C. § 78m (b) (2) (B).

14 Vgl. IIA (2009), pp. 17, 24.

15 Vgl. IDW (2002), S. 1176.

16 Vgl. Bundesministerium der Justiz (2009b).

griffsberechtigten Personen (§ 4g (2) BDSG) und die Verpflichtung dieser Personen auf das Datengeheimnis (§ 5 BDSG). Werden Datenbestände zum Zwecke der Analyse an Dritte weitergeleitet, so ist der Auftraggeber für die Einhaltung der Vorschriften des BDSG verantwortlich. Insbesondere fordert hier das BDSG die schriftliche Fixierung der technischen und organisatorischen Auftragsbedingungen sowie die Überprüfung deren Einhaltung durch den Auftraggeber beim Auftragnehmer.

Die für eine Analyse benötigten personenbezogenen Daten sollten auf den unbedingt – und vorab eindeutig definierten – erforderlichen Umfang beschränkt und nach Abschluss der Untersuchung unverzüglich gelöscht werden.

Die rechtzeitige Einbeziehung der Personal- und der Rechtsabteilung in das Vorhaben einer Datenanalyse mit personenbezogenen Daten ist notwendig. Dies dient auch der Vorbereitung eventueller personeller Konsequenzen bei positiven Analyseergebnissen. Die Interne Revision sollte dabei die Rechtmäßigkeit des Datenanalyse-Vorhabens absichern und die weitere Verwendung verdachtsbegründender Informationen bei den zuständigen Fachstellen gewährleisten. Ebenso ist die rechtzeitige Einbeziehung der Mitarbeiter-Vertretung zu empfehlen und die Beachtung eventuell bestehender Betriebsvereinbarungen erforderlich – dies gilt insbesondere für den Fall tatsächlich aufgedeckter wirtschaftskrimineller Handlungen durch Mitarbeiter und dann zu beachtende rechtliche Fristen.

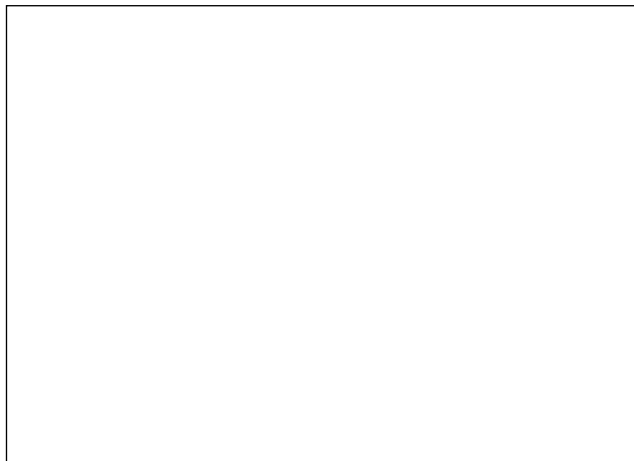
## 5. Fazit und abgeleitete Empfehlungen für die Interne Revision

Die Analyse von Datenbeständen gehört seit der Einführung elektronischer Datenverarbeitung zum Standard-Repertoire einer Internen Revision und wird es auch in der Zukunft bleiben. Wesentliche Argumente sind die deutlich höhere Effizienz bei analytischen Prüfungen und die Notwendigkeit, wirtschaftskriminelle Handlungen möglichst systematisch und frühzeitig zu erkennen.

Auch für die Analyse personenbezogener Daten sind IT-Tools aufgrund der häufig erheblichen Komplexität von Datenbeständen unverzichtbar. In diesem speziellen Fall ist allerdings die Beachtung des BDSG unabdingbar. Daher ist die rechtzeitige Einbeziehung des zuständigen Datenschutzbeauftragten im Hause zu empfehlen – dieser kann im Zweifelsfall auch Hilfestellung geben, ob Mitarbeiter bei personenbezogenen Datenanalysen über das Vorhaben informiert werden müssen (u. a. § 33 BDSG).

Folgende Vorgehensweise im Zusammenhang mit der Analyse personenbezogener Daten empfiehlt das DIIR seinen Mitgliedern:

- (1) Es sollten im Unternehmen eindeutige Regeln – von der Unternehmensleitung verabschiedet und bei Nichtbeachtung sanktioniert – bestehen, anhand derer verbindliche Verhaltensweisen und Prozeduren bspw. im Verhältnis zu Lieferanten oder Kunden definiert werden. Eventuell kann ein Verhaltenskodex erstellt werden. Diese Regelungen bilden den Maßstab für die ordnungsmäßige Einhaltung bestehender Prozeduren. Dabei sollte die Unternehmensleitung auch ihre Position zur Wirtschaftskriminalität formulieren, nachvollziehbar kommunizieren und die Bedeutung möglicher präventiver und kurativer Maßnahmen im Rahmen des IKS betonen.
- (2) Die Interne Revision sollte sich über die Prüfungsplanung von der Unternehmensleitung das Mandat zur Durchführung personenbezogener Datenanalysen einholen. Sehen interne Regularien dies vor, sollte auch der Prüfungsausschuss bzw. der Aufsichtsrat informiert werden.
- (3) Sind nicht bereits unter (2) entsprechende Freigaben erfolgt, sollte bei personenbezogenen Datenanalysen unter Information an die Unternehmensleitung festgelegt werden, dass diese zur Wahrung berechtigter Interessen des Unternehmens/der verantwortlichen Stelle dienen und damit das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung überwiegen (§ 28 BDSG). Der Schutz des Unternehmensvermögens und die Verhinderung und Aufdeckung von Vermögensschädigungen ist hierbei ein überragendes Argument – insbesondere wenn ein Betrugsverdacht vorliegt.
- (4) Der Umfang der Datenanalyse sollte vorab eindeutig definiert, abgegrenzt und dokumentiert werden. Wenn möglich sollte ein zu untersuchender Personenkreis definiert werden (bspw. Abteilung/Funktion).



- (5) In allen Fällen sollten die Daten anonymisiert/pseudonymisiert werden<sup>17</sup>.
- (6) Der angestrebte Untersuchungsprozess bei der personenbezogenen Datenanalyse sollte vorab abgestimmt und dokumentiert werden (eventuell in einer Verfahrensweisung). Die Abstimmung sollte mit der Personal- und – falls die Interne Revision nicht über eigene entsprechende Ressourcen verfügt – der Rechtsabteilung sowie dem Datenschutzbeauftragten und der Mitarbeiter-Vertretung erfolgen. Die Abstimmung mit der Mitarbeiter-Vertretung wird empfohlen in Zusammenhang mit den §§ 87 Abs. 1 Nr. 6, 90 Abs. 2 BetrVG; sie kann außerdem dazu dienen, bei positiven Analyseergebnissen bestehende rechtliche Fristen einzuhalten (insbesondere § 626 BGB – zweiwöchige Frist bei Verdachtskündigungen).
- (7) Bei der Konkretisierung von Verdachtsmomenten aus einer personenbezogenen Datenanalyse (Vermögensschädigung durch Mitarbeiter) sollte – sofern für diese Fälle nicht bereits Prozeduren definiert sind – das weitere Vorgehen mit den zuständigen Fachstellen abgestimmt werden. Dies betrifft bspw. die Personalabteilung und – falls die Interne Revision des Hauses selbst keine relevante juristische Expertise hat – auch die Rechtsabteilung. Bei der Konkretisierung von Verdachtsmomenten mit möglichen arbeitsrechtlichen Konsequenzen ist außerdem die Mitarbeiter-Vertretung einzubeziehen (siehe hierzu auch Fristenregelung unter 6, im Besonderen § 102 BetrVG mit § 626 BGB).
- (8) Bei der Einbeziehung externer Dienstleister zu Analysezielen ist darauf zu achten, dass
  - ◆ schriftliche Vereinbarungen (inklusive Informationsschutzvereinbarung) geschlossen werden
  - ◆ der Auftragsumfang eindeutig und datenschutzkonform definiert wird

- ◆ der Dienstleister die Einhaltung legaler Mittel und der relevanten Datenschutzbestimmungen schriftlich zusichert (inklusive eventuell einbezogener Subunternehmen)
  - ◆ eventuelle Subunternehmen dem Auftraggeber schriftlich zur Kenntnis gebracht werden und er deren Einbeziehung zustimmt
  - ◆ keine Weitergabe der verwendeten Daten an Dritte erfolgt.
- (9) Die zur Analyse verwendeten Daten, die keine Verdachtsmomente begründen, sind unverzüglich und nachvollziehbar zu löschen.
  - (10) Für den Fall, dass der Internen Revision derartige Prüfungen untersagt werden, sollte der Leiter der Internen Revision dies angemessen dokumentieren.

#### Literaturverzeichnis

- Bundeskriminalamt (BKA): Wirtschaftskriminalität – Bundeslagebild 2007 (pressefreie Kurzfassung), Wiesbaden, o. Datum.
- Bundesministerium der Justiz (BMJ 2009a): Gesetz über das Kreditwesen (Kreditwesengesetz – KWG) in der Fassung vom 12. 3. 2009, Berlin, 2009.
- Bundesministerium der Justiz (BMJ 2009b): Bundesdatenschutzgesetz (BDSG) in der Fassung vom 5. 2. 2009, Berlin, 2009.
- Deutscher Bundestag: Drucksache 16/10067 vom 30. 7. 2008, Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz – BilMoG), Berlin, 2008.
- Euler Hermes Kreditversicherungs-AG: Wirtschaftskriminalität – die verkannte Gefahr, Hamburg, 2008.
- Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW): Abschlussprüfung bei Einsatz von Informationstechnologie, in: WPg 2002, Heft-Nr. 21/2002, Düsseldorf, 2002.
- Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW): Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken, in: WPg 2006, Heft-Nr. 22/2006, Düsseldorf, 2006.
- PricewaterhouseCoopers (PwC): Wirtschaftskriminalität 2007 – Sicherheitslage der deutschen Wirtschaft, Frankfurt, 2007.
- Schartmann, B./Lindner, M.: Prüfung des Internen Kontrollsystems (IKS) durch die Interne Revision (IR), in: Lück, W. (Hrsg.), Zentrale Tätigkeitsbereiche der Internen Revision, Berlin, 2006, S. 33–61.
- The Institute of Internal Auditors (IIA): A World in Economic Crisis: Key Themes for Refocusing Internal Audit Strategy, Altamonte Springs, Fla., 2009.
- U. S. Department of Justice: The Foreign Corrupt Practices Act, Washington, 1998.
- U. S. Securities and Exchange Commission (SEC): Final Rule – Management’s Report on Internal Control Over Financial Reporting and Certification Disclosure in Exchange Act Periodic Reports, Washington, 2003.

<sup>17</sup> Vgl. Bundesministerium der Justiz (2009b): § 3 (6) „Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbarer natürlichen Person zugeordnet werden können.“ (6a) „Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.“