

# Konfliktfeld „Compliance und Datenanalysen“

## Fach- und sachgerechte Datenanalysen unter Beachtung gesetzlicher Randbedingungen

### 1 Daten und Skandale

Das in der Überschrift bezeichnete Thema verknüpft zweckmäßige Aspekte revisionsbezogener Datenanalysen mit dem Compliance-Begriff. Es reflektiert insoweit häufig zitierte und öffentlichkeitswirksame Vorgänge bei Lidl, Telekom und Deutsche Bahn. So skizzierte u. a. die Süddeutsche Zeitung mit dem Aufmacher „173.000 Mitarbeiter in der Spitzel-Falle“ Bahnrevisoren als persönlichkeitsgestörte, voyeuristische Schnüffler. Glücklicherweise hat die sich hieraus entwickelnde Wahrnehmung zu Datenanalysen in der Revisionsarbeit wenig mit der täglichen Prüferpraxis gemein, wie ein nüchterner Blick auf die einzelnen Sachverhalte zeigt:

- Lidl  
Die kritisierte Beobachtung von Betriebsangehörigen erfolgte ohne Revisionsbegleitung durch beauftragte Detekteien. Diese erstellten schriftliche Persönlichkeitsprofile und Integritätseinschätzungen.
- Telekom  
In diesem Fall wurden Verbindungsdaten privater Mobiltelefone von Journalisten, Aufsichtsratsmitgliedern sowie einigen Betriebsräten mittels Prüfsoftware ausgewertet. Die Analysen erfolgten im Auftrag der Konzernsicherheit durch die Firma eines Berliner Wirtschaftsprüfers.
- Deutsche Bahn  
Detekteien waren mit Privatermittlungen bis hin zur Aufhellung privater Kontenbewegungen verdächtiger Bahnmitarbeiter und (betriebsfremder) Angehöriger beauftragt. Unabhängig hiervon und zusätzlich veranlasste die Revision einen automatisierten Kontenabgleich bei Lieferanten und Beschäftigten. Auftragnehmer war ebenfalls die hierauf spezialisierte Gesellschaft des bereits für die Telekom tätigen Berliner Wirtschaftsprüfers.

Aus der vorstehenden Darstellung wird deutlich, dass sich kritikwürdige, in die Privatsphäre von Mitarbeitern wirkende Untersuchungen überwiegend fern von Revisionsstellen und deren Arbeit abgespielt haben. Gleichwohl wurde der einzig zu Datenanalysen in Verbindung stehende Abgleich von Beschäftigten- sowie Kreditoren-Positionen mit den übrigen Taten gleichgestellt und als „Datenscreening“ bzw. „Schnüffelpraxis“ stigmatisiert. Die Folgen sind evident und reichen bis hin zur Gestaltung spezieller gesetzlicher Randbedingungen für prüferische Datenauswertungen, denen wir uns in den nachfolgenden Ausführungen über Zweckmäßigkeitsbetrachtungen hinaus zuwenden.

### 2 Mehr als man denkt

Stürmische Zeiten befördern erfahrungsgemäß einfache Lösungsvorschläge. Warum, so fragen sich viele berufene „Experten“, kann sich die Revision nicht einfach auf die Auswertung „geschäftlicher“ Daten beschränken? Tatsächlich sind digitale Informationen zu Mitarbeitern in der sozio-technischen Organisationsform eines Unternehmens tief mit weiteren betrieblichen Datenstrukturen verwoben. Über die offensichtlichen Personalmodule hinaus finden sie sich z.B. als Arbeitsaufzeichnungen in der Kostenrechnung. Für die Erstattung betriebsbedingter Aufwendungen werden Personalkreditoren in der Finanzbuchhaltung angelegt. Das Rechnungswesen steuert Belegverarbeitungen über Buchhalterschlüssel. Die Anlage von Kundendaten in der Vertriebsapplikation wird ebenso mit dem Personalkennzeichen festgehalten, wie Preis- oder Mengenänderungen.

Wohin man auch blickt, stets hinterlassen Beschäftigte an den Schnittstellen zur Informationsverarbeitung ihren digitalen Fingerabdruck innerhalb der DV-Systeme. Unternehmensdaten spiegeln insoweit reale Betriebsprozesse einschließlich hierin involvierter Akteure, zu denen unzweifelhaft die Beschäftigten zählen. Die Vorstellung, eine Interne Revision könnte sich konstruktiv mit „Geschäftsdaten“ einschließlich hieraus ablesbarer Risiken auseinandersetzen ohne hierbei mit Mitarbeiterinformationen in Berührung zu kommen, erweist sich vor diesem Hintergrund als Illusion.

### 3 Revisionsziele und -werkzeuge

Ein fach- und sachgerechter Einsatz von Prüfungshilfsmitteln muss sich an Anwendungsszenarien sowie hiermit verfolgten Zielen messen lassen. Bei Prüfsoftware handelt es sich, auch wenn der Einsatz durch die steuerliche Betriebsprüfung in den letzten Jahren als revolutionäres Ereignis stilisiert wurde, eher um ein tradiertes Werkzeug. Sie ergänzt seit über 40 Jahren den bescheidenen Werkzeugkasten der Internen Revision, ohne dass sich hierbei besondere Probleme gezeigt hätten. Deren Ziele und Arbeitsweise haben sich in diesem Zeitraum bei genauerer Betrachtung auch nur unwesentlich geändert. Primäre und wichtigste Aufgabe ist die Unterstützung des Managements bei der Kontingenzbewältigung.

Kaum eine Führungskraft könnte mit den vielfältigen, weithin unbestimmten und unüberblickbaren Einflussfaktoren auf ein Unternehmen umgehen, wenn diese nicht vorab unter wesentlicher Mitwirkung von in- und externen Prüfungsstellen in kalkulierbare Risiken (Auftragsrisiken, Kontrahierungsrisiken, Marktrisiken, Kontrollrisiken, Betrugsrisiken etc.) umgedeutet würden. Dieses Erfordernis trifft gleichermaßen einzelne Geschäftsführer wie die Gesellschaft als Ganzes. Es findet seinen Niederschlag in Erwartungen, Standards und gesetzlichen Vorgaben zur „Risikovorsorge“ oder „Prüfungsqualität“. So geht z.B. die Finanzverwaltung selbstverständlich davon aus, dass ein „testierter“ Jahresabschluss mit guter Wahrscheinlichkeit als zutreffende Grundlage der Steuerfestsetzung herangezogen werden kann.

Die Interne Revision erfüllt die geschilderte Aufgabe, in dem sie sich mit überschaubarem Aufwand

- einen Überblick über den Realitätsgehalt betrieblicher Aufzeichnungen verschafft, während sie *Prüfungen in Stichproben* mit detektivischen oder zufallsbasierten Auswahlverfahren durchführt,
- dazu beiträgt, den Handlungsspielraum der Mitarbeiter in einem auf Vertrauen begründeten Arbeitsumfeld an Regeln zu orientieren,
- präventiv Kontrollbewusstsein dadurch fördert, dass sie außergewöhnliche Vorfälle findet und mit hierfür Verantwortlichen erörtert,
- konkrete Untersuchungen zu unbeabsichtigten oder beabsichtigten Regelverletzungen durchführt (Einschätzung von Fehlerquellen sowie forensische Untersuchungen).

In allen diesen Bereichen spielen „Prüfsoftware“ und „Datenanalysen“ eine wesentliche Rolle. Da sich darüber hinaus betriebliche und persönliche Daten, wie bereits dargestellt, kaum zuverlässig segregieren lassen, steht, auch wenn gesetzliche Bestimmungen etwas anderes insinuiert, die Realität einfachen Handlungsempfehlungen zu „compliance-konformen“ Auswertungstechniken häufig entgegen.

### 4 Problembereiche

Lösungsalternativen für fach- und sachgerechte Datenauswertungen unter Einbeziehung rechtlicher Rahmenbedingungen können sich nur begrenzt auf die sophistische Auslegung von Gesetzestexten stützen. Sie müssen vielmehr die Vielfalt geschäftlicher Erscheinungen widerspiegeln und sich in der Praxis bewähren. Dieses erfordert eine grundlegende Erörterung sowie die gegenseitige Berücksichtigung widersprüchlicher Interessen:

- Verschränkung

Der Intim- und Privatsphäre von Personen wird in unserem Kulturkreis ein außerordentlicher Wert beigemessen. Sie endet nicht an der Unternehmenspforte sondern wird im übertragenden Sinne seitens der Beschäftigten in den Betrieb hineingetragen, wo sie sich u.a. mit geschäftlichen Informationsflüssen vermischt. Deutlich wird es überall dort, wo sich ein Arbeitnehmer betrieblicher Infrastruktur für private Verrichtungen

- private Telefonate,
- persönlicher E-Mail-Verkehr,
- Surfen im Internet,
- Erstellen familiärer Korrespondenz auf dem Arbeitsplatz-PC,
- Kopiervorgänge für eigene Zwecke

bedient. Hinzu kommen private Ein- und Verkäufe, Nutzung von Firmenrabatten, Bonussystemen und ähnlichem, wodurch sich der Status des Arbeitnehmers um den des Debtors, Kreditors,

Konteninhabers, Darlehensnehmers, Mieters etc. erweitert. Bereits eine einfache wirtschaftliche Auswertung zu Firmenfahrzeugen, die gleichermaßen geschäftlich wie privat genutzt werden können, führt somit in persönliche Bereiche. Mit etwas Phantasie lässt sich das Spannungsfeld zwischen dem Wunsch nach informationeller Selbstbestimmung von Mitarbeitern und unternehmerischen Erfordernissen erkennen. Dem könnten sich Betriebe wie Arbeitnehmer nur durch die konsequente Trennung beider Sphären entziehen, die jedoch mit unterschiedlichen Argumenten ebenfalls weitgehend ausgeschlossen wird.

- Ambivalenz

Die *persönliche Betroffenheit* Beschäftigter bei der Aufbereitung geschäftlicher Daten, die bis in die Privatsphäre hineinreichen können, ist unmittelbar nachvollziehbar. Dies gilt gleichermaßen für Befindlichkeiten unbescholtener Arbeitnehmer, wie für solche, welche betriebliche Ressourcen nutzen, um sich an dem Geschäftsvermögen ihres Arbeitgebers zu bereichern. Dieser möchte der Gesetzgeber entsprechen. Widerstreitende Interessen und Ambivalenz offenbaren sich jedoch dort, wo aus einer *gesellschaftlichen Sicht* heraus von Verantwortlichen gleichzeitig

- funktionierendes Risikomanagement,
- wirksame interne Kontrollsysteme,
- taugliche Maßnahmen zur Verhinderung von Mitarbeiterkriminalität, Betrug und Bilanzfälschungen

verlangt werden. Alle aufgeführten Risikofaktoren, vom Fehler bis zum Betrug, haben unzweifelhaft mit Menschen und hier u.a. mit Arbeitnehmern zu tun. Dieses gilt es beim Einsatz von Hilfsmitteln, die seitens der Internen Revision für Prüfungs- und Kontrollzwecke angewendet werden, zu berücksichtigen.

- Erwartungslücke

Viele betriebliche Prüfungsstellen überlegen angesichts der bereits angesprochenen Imponderabilien, es bei der Analyse entkernter, aller persönlicher Informationen bereinigter Geschäftsdaten zu belassen oder auf das Arbeitsmittel Prüfsoftware ganz zu verzichten?

Dieses erscheint mit einigem wirtschaftlichen Aufwand durchaus vorstellbar. Angesichts der digitalen Durchdringung realer Betriebsprozesse wäre hiermit jedoch eine unausgesprochene Fokussierung auf den technischen Aspekt des sozio-technischen Gebildes „Unternehmen“ verbunden. Viele *Abweichungen* von Regeln:

- Überschreitung von Unterschriftsgrenzen bei bestimmten Betragshöhen,
- verbotenes Ausschleusen von Firmenvermögen über Mitarbeiterkonten,

die mit Personen oder Personengruppen verbunden sind, ließen sich aus verbleibenden Daten nicht mehr herausfiltern. Gleiches gilt für die Suche nach *Ursachen* ermittelter Abweichungen:

- welche Stelle / Mitarbeiter verursacht außergewöhnliche Inventur- oder Kassendifferenzen,
- sind Fehler auf unzureichende Prozesskenntnisse oder Schulungen von Mitarbeitern zurückzuführen.

Revisionen würden sich weitgehend ohne Rücksicht auf die Wirksamkeit ihrer Prüfungen im Wesentlichen auf deren formale Aspekte beschränken. Die präventive Wirkung von Datenanalysen könnte sich ebenfalls kaum einstellen. Konsequenterweise wäre in diesem Zusammenhang offensiv darauf hinzuweisen, dass die derzeit hohen Erwartungen an die Arbeit in- und externer Prüfungsstellen reduziert werden sollten.

- Schuld hat immer der Computer

Mit vorstehender Schlagzeile leitete eine überregionale Tageszeitung einen Artikel über die Bilanzierungspanne in Höhe von 56 Mrd. Euro-Panne bei der verstaatlichten Immobilienbank Hypo Real Estate (HRE) ein. Gefolgt von dem Hinweis „*Kein Mensch will die Verantwortung für die Fehlbuchungen der HRE tragen*“. Es besteht offensichtlich ein fundamentales gesellschaftliches Interesse daran, Fehler, Risiken, Pannen und Unregelmäßigkeiten auf *handelnde Personen* zurückzuführen. Dies gilt zumindest dort, wo Vertrauen und Verantwortung ineinander greifen sollten. Wenn eine solche Rückführung auf Personen ausschließlich als Eingriff in die Privatsphäre bzw. zu kritisierende Verhaltens- und Leistungskontrolle eingeordnet wird, könnten Verantwortliche zumindest mittels Datenanalysen kaum mehr identifiziert werden.

- Wer traut wem?

Die öffentlich artikulierte und auch seitens der Politik nachdrücklich vorgetragene Forderung, betriebliche Prüfungsstellen sollten sich bei der Auswertung von Unternehmensdaten dort einschränken, wo private Interessen von Arbeitnehmern entgegenstehen, gilt offensichtlich nicht für das Auswertungsinteresse nachgeordneter, staatlicher Prüfstellen.

So hat die Finanzverwaltung keine Probleme damit:

- persönliche Arbeitnehmerdaten einschließlich Urlaubszeiten und -ausgaben mit betrieblichen Reisekostenabrechnungen abzugleichen, um hieraus gegebenenfalls Unregelmäßigkeiten zu identifizieren,
- mögliche Scheinrechnungen im Lieferantenbereich einschließlich einer damit verbundenen Umsatzsteuerverkürzung dadurch zu identifizieren, dass Kontenverbindungen von Lieferanten sowie von Arbeitnehmern mittels Prüfsoftware automatisch abgeglichen werden.

Je nach Motivation der Auswertung:

- Betrugsverhinderung und -aufdeckung           Interne Revision
- Erzielung steuerlicher Mehrerlöse               Steuerliche Betriebsprüfung

erscheint ein identisches prüferisches Vorgehen unter Einsatz gleicher Werkzeuge somit unterschiedlich kritikwürdig. Unternehmensverantwortliche sehen sich so gegebenenfalls seitens staatlicher Stellen mit den Folgen eines derart aufgehellten Mitarbeiterdeliktes konfrontiert, ohne dass dieses von der Internen Revision im Vorfeld hätte aufgeklärt werden dürfen.

- Begrifflichkeiten

Zu einem von der Internen Revision selbst zu verantwortenden Problembereich im Zusammenhang mit prüferischen Datenauswertungen gehört sicherlich die weitgehend empathiefreie und fehlerhafte Verwendung unangemessener, missverständlicher oder Angst erzeugender Begriffe. Hierzu gehören u.a. „Massendatenanalysen“, „Screening“, „Rasterfahndung“, „Data-Mining“, „Datenscan“, „Continuous Auditing“, „Continuous Control Monitoring“, die nur am Rande mit der vorherrschenden Anwendung von Revisionssoftware zu tun haben, allerdings bestens geeignet sind, ein unzutreffendes Bild betrieblicher Prüfung in der Öffentlichkeit zu verstärken.

Ob die überwiegend hiermit in Verbindung gebrachte Prüfsoftware ACL (Audit Command Language) oder IDEA (Interactive Data Extraction and Analysis) für einen solchen Einsatz besonders gut geeignet ist, darf trotz entgegenstehender Werbung ernsthaft bezweifelt werden. Hierfür wurde sie auch nicht konzipiert. Bereits die Bezeichnungen beider Programme verweisen auf die ursprüngliche Intention, nach der sich ein Revisor die Auswahl zu prüfender Vorgänge über eine interaktive, dialogorientierte und schrittweise Auseinandersetzung mit den Unternehmensdaten erarbeiten sollte. Dieser Weg, bei welchem er seine prüferische Erfahrung auf digitale betriebliche Informationen appliziert, ist das Ziel und weniger die phantasielose Aufbereitung von „Massendaten“ nach einfach programmierten Regeln (Continuous Auditing), die je nach Betrachtung zu viel oder zu wenig Findings für den Abgleich mit der Realität (Prüfung) erzeugen.

Für viele der aufgeführten Problembereiche bieten Gesetze alleine keine befriedigende Lösung. Protagonisten, die heute vornehme Zurückhaltung der Revision einfordern, werden sich nach dem nächsten Korruptionsskandal über unzureichende Prüfungen äußern. In einer offensiven öffentlichen wie betrieblichen Diskussion sollten daher die Motive für Revisionsarbeit aufgezeigt und um gangbare Lösungen geworben werden.

## **5 Ein Blick in die Gesetze**

In eine Beurteilung betrieblicher Datenverarbeitung einschließlich von der Revision eingesetzter Software können unter Compliance-Gesichtspunkten (gesetzestreue Anwendung) unterschiedlichste gesetzliche Bestimmungen herangezogen werden. Die nachfolgenden Ausführungen beziehen sich im Zusammenhang mit Datenanalysen u. a. auf viel diskutierte Bestimmungen des Betriebsverfassungsgesetzes sowie einzelne Paragraphen des *novellierten* Bundesdatenschutzgesetzes.

- Betriebsverfassungsgesetz

Ein Blick in die Bestimmungsregelungen des Betriebsverfassungsgesetzes zeigt, dass insbesondere die *Mitbestimmung des Betriebsrates im Rahmen der Verhaltens- und Leistungskontrolle* (§ 87 Abs. 1 Nr. 6 BetrVG) zu beurteilen ist.

Bei nüchterner Betrachtung sind die in Prüfsoftware integrierten Analyseverfahren unzweifelhaft dazu geeignet, eine Verhaltens- und Leistungskontrolle mittels personenbezogener Arbeitnehmerdaten zu ermöglichen. Angesichts der bereits erörterten Verschränkung von Arbeitnehmer- und Geschäftsdaten wird dieses jedoch ebenso für jedes weitere Datenanalyse- und Aufbereitungsprogramm, beginnend bei Standardauswertungen von Buchhaltungssoftware, über Datenbanksysteme bis hin zu Excel-Tabellen der Fall sein. Es kommt daher entscheidend auf die konkrete Anwendung der Programme und die inhaltliche Ausgestaltung der Datenquellen an. Ein Mitbestimmungserfordernis für Revisionssoftware im Vergleich zu den weiter zitierten Programmsystemen ergäbe sich somit nicht alleine aus den Eigenschaften des Programms sowie dessen Einsatz bei allgemeinen revisionsbezogenen Analysen, sondern insbesondere dann, wenn Auswertungen im Hinblick auf besondere personelle Merkmale erfolgen. Dieses dürfte zumindest bei forensischen Datenanalysen ausnahmslos der Fall sein.

Mitbestimmung umfasst hierbei die *Überwachungsrechte* der Personalvertretung z.B. zur adäquaten Einhaltung von (Daten-)Schutzgesetzen (§ 80 Abs. 1 Nr. 1 BetrVG) sowie hierauf gerichtete *Informationsrechte* (§80 Abs. 2 Nr. 1 BetrVG).

Zusammenfassend ergibt sich hieraus das Erfordernis, den Betriebsrat umfassend zu *unterrichten*, wenn mittels Revisionssoftware Geschäftsdaten mit mitarbeiterbezogenen Merkmalen unter Einhaltung einschlägiger Datenschutzbestimmungen z. B. anonymisiert ausgewertet werden. *Mitbestimmungsrechte* sind darüber hinaus im Einzelfall bei Auswertungen zu konkreten Personen zu berücksichtigen. Es erscheint daher sinnvoll, mit der Personalvertretung eine grundsätzliche Regelung über generelle und einzelfallbezogene Aspekte revisionsbezogener Datenanalysen z.B. in Form einer Betriebsvereinbarung zu suchen.

- Bestimmungen des Bundesdatenschutzgesetzes

Als personenbezogene Daten gelten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person („Betroffene“ i. S. § 3 Abs. 1 BDSG). Deren Verarbeitung, Speicherung oder Übermittlung ist lediglich zulässig, sofern hiervon Betroffene ausdrücklich eingewilligt, sich Bearbeitung aus dem Vertragszweck ergibt oder ein sonstiges berechtigtes Interesse an der Verarbeitung dieser Daten besteht. Arbeitnehmerdaten, wie weitere z.B. zu Debitoren oder Kreditoren sind hier einzuordnen und in der Vergangenheit wurden kaum ernstliche Zweifel dahingehend geäußert, dass deren gelegentliche Einbeziehung in prüferische Auswertungen z. B. zum Zwecke der Betrugsprävention ein berechtigtes betriebliches Interesse darstellt.

Nach den Eingangs bezeichneten Vorfällen folgte in § 32 BDSG unter dem Stichwort „Beschäftigtendatenschutz“ eine spezielle Regelung für Arbeitnehmer. Hier heißt es:

*„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.“*

Die aufgeführte Bestimmung wird einhellig als misslungen bezeichnet. Zwar tangiert sie offensichtlich nicht ganz allgemeine Datenanalysen. Datenabgleiche mit präventiver Wirkung zur Betrugsverhinderung oder Stärkung des Internen Kontrollsystems werden jedoch torpediert, da sie von einem konkreten „Anfangsverdacht“ abhängig gemacht werden. Offensichtlich verwechselt

der Gesetzgeber hier „Aufdeckung“ und „Untersuchung“. *Vorbeugende (verbotene) Datenanalysen* dienen durch die Erzeugung von Kontrollbewusstsein der Betrugsverhinderung bzw. der Aufhellung möglicher Verdachtsmomente. Liegen letztere im Ergebnis anschließend vor, sind die Schäden erfahrungsgemäß bereits eingetreten und weitere (erlaubte) Datenauswertungen mit Bezug zur verdächtigten Person häufig überflüssig!

Die vorbezeichnete Kritik führte zu einem neuen differenzierten Gesetzentwurf. Dieser beschäftigt sich in den §§ 32a-l überwiegend mit Datenerhebungen, Beobachtungen, Ortungen oder Nutzung von Verbindungsdaten bei betrieblichen Kommunikationsmitteln. Datenanalysen sind lediglich von einigen Bestimmungen betroffen, wie die nachfolgende Übersicht zeigt:

<u>Direkter Bezug zu Datenanalysen</u>	<u>Sonstige oder Sonderuntersuchungen</u>
32d Datenverarbeitung und –nutzung im Beschäftigungsverhältnis	32 Datenerhebung vor Begründung eines Beschäftigungsverhältnisses
32e Datenerhebung ohne Kenntnis des Beschäftigten zur Aufdeckung und Verhinderung von Straftaten und anderen schwerwiegenden Pflichtverletzungen im Beschäftigungsverhältnis	32a Ärztliche Untersuchungen und Eignungstests vor Begründung eines Beschäftigungsverhältnisses
32j Unterrichtungspflichten	32b Datenverarbeitung und -nutzung vor Begründung eines Beschäftigungsverhältnisses
32l Einwilligung, Geltung für Dritte, Rechte der Interessenvertretungen, Beschwerderecht, Unabdingbarkeit	32c Datenerhebung im Beschäftigungsverhältnis
	32f Beobachtung nicht öffentlich zugänglicher Betriebsstätten mit optisch- elektronischen Einrichtungen
	32g Ortungssysteme
	32h Biometrische Verfahren
	32i Nutzung von Telekommunikationsdiensten
	32k Änderungen

Aus den hier aufgeführten Regelungen lassen sich folgende Kernsätze extrahieren:

- Der Arbeitgeber darf Beschäftigungsdaten verarbeiten und nutzen, soweit dies zur Erfüllung der originären Erhebungszwecke sowie andere Zwecke, für die der Arbeitgeber sie erheben dürfen, erforderlich ist.
- Beschäftigungsdaten dürfen zur Aufdeckung von Straftaten oder anderer schwerwiegender Pflichtverletzungen in anonymisierter oder pseudonymisierter Form mit weiteren betrieblichen Daten abgeglichen werden.
- Im konkreten Verdachtsfall darf der vorerwähnte Abgleich mit personalisierten Beschäftigungsdaten erfolgen.
- Die Verarbeitung personenbezogener Daten zu Revisionszwecken muss verhältnismäßig sein.
- Durch die automatisierte Auswertung dürften sich keine Persönlichkeitsprofile der Beschäftigten ergeben.
- Beauftragte Dritte dürfen Beschäftigungsdaten ausschließlich nach den vorstehend aufgeführten Prinzipien verarbeiten.
- Es bestehen Unterrichtungspflichten gegenüber dem Datenschutzbeauftragten sowie den Beschäftigten.

Schaut man auf den korrigierten Gesetzesentwurf und die vorstehend abgeleiteten Grundsätze, so lässt sich mit Blick auf die Zweckbindung selbst bei enger Auslegung herleiten, dass zulässige Leistungs- und Verhaltenskontrollen z.B. zur Einhaltung gesetzlicher oder betrieblicher Regeln sowie präventive Prüfungen unter Einbeziehung von Prüfsoftware weiterhin möglich, wenn nicht gar geboten wären. Dies gälte gleichermaßen für spezielle Datenabgleiche unter Einbeziehung personeller Merkmale (z. B. Kontoverbindungen, Telefonnummern), wenn direkte Identifikationsdaten anonymisiert oder pseudonymisiert würden.

Datenanalysen dürften darüber hinaus besonders geeignet sein, die hiermit verbundenen Zwecke wirtschaftlich und somit *verhältnismäßig* sicherzustellen.

Über die bisher überwiegend in den Unternehmen praktizierte Handhabung ergäbe sich bis auf den Aspekt der Anonymisierung / Pseudonymisierung keine wesentliche Änderung. Zumindest allgemeine Unterweisungen der Beschäftigten über entsprechende Datenauswertungen wurden bisher bereits vielfach aus Gründen der Generalprävention z.B. durch Aushänge praktiziert oder in Betriebsvereinbarungen geregelt.

Die unter Verhältnismäßigkeitsgrundsätzen oftmals geforderte Einschränkung von Datenabgleichen z.B. zwischen den Konteninformationen von Mitarbeitern und Lieferanten ist sowohl unter fachlichen als auch unter gesetzlichen Gesichtspunkten wenig zielführend. Auf welche Beschäftigtengruppen sollte in diesem Fall eine entsprechende Einschränkung erfolgen:

- Den Einkäufer, welcher Bestellvorgänge bei gegebenenfalls fiktiven Lieferanten vornimmt?
- Die Mitarbeiter, welche Bedarfsmeldungen an den Einkauf mit Vorgaben für bestimmte Lieferanten weitermelden?
- Solche betrieblichen Stellen, die dezentrale Beschaffungsvorgänge auslösen können?
- Mitarbeiter der Kreditorenbuchhaltung, die Scheinrechnungen auf fiktive Lieferanten kontieren können?
- Beschäftigte, die in der Lage sind, weitere Kreditorenstammdaten z.B. für abweichende Zahlungsempfänger zu pflegen?

In jedem Einzelfall würde die spezielle Auswahl die Mitarbeiter der beschäftigten Stellen einem erhöhten Manipulationsverdacht aussetzen, der jedoch gerade nicht Grundlage dieser präventiv wirkenden Analyse sein soll. Wenn die personenbezogenen Merkmale überdies in verschlüsselter Form in die Bewertung einbezogen werden, gibt es keine nachvollziehbare Begründung für die geforderte Eingrenzung.

Eine differenzierte Beurteilung erfordert die *Analyse personalisierter Daten im konkreten Verdachtsfall*. Spätestens hier ist der Betriebsrat nach den nun vorliegenden Bestimmungen (Überwachungsrecht bei der Anwendung von Schutzgesetzen) zwingend einzubeziehen. Ferner ist in diesem Fall eine Einzelabwägung zur Verhältnismäßigkeit der Auswertung unerlässlich. Die Interne Revision sieht sich hier gegebenenfalls in der Rechtfertigungspflicht, warum alternative, mildere Prüfungsformen nicht gegebenenfalls zu einem vergleichbaren Urteil hätten führen können. Zu diesem Zweck sind die näheren Umstände der *verdachtsabhängigen, personalisierten Auswertung* nachvollziehbar zu dokumentieren. Dies gilt gleichermaßen für die eigene Arbeit, wie für die Arbeit sachverständiger Dritter, die entsprechende Analysen nach Vorgaben der Internen Revision und ggf. in deren Verantwortung (Grundsatz der Auftragsbindung) durchführen.

Insgesamt ist festzustellen, dass nach dem neuen praxisnahen Regelungsentwurf allgemeine, fehlerorientierte Datenanalysen weitgehend unverändert vorgenommen werden können, während Prüfungen im Verdachtsfall ein kontrollierbares und formalisiertes Vorgehen unter Einschaltung weiterer Überwachungsstellen sowie der Arbeitnehmervertretung erfordern. Hierauf wird nachfolgend näher eingegangen.

## 6 Darstellung praktischer Handlungsalternativen

Nach ausführlicher Erörterung widerstreitender Anforderungen und Interessen im Revisionsumfeld sowie den gesetzlichen Randbedingungen von prüfungsbezogenen Datenanalysen sollten nun noch ein abschließender Blick auf mögliche Handlungsalternativen geworfen werden. Es handelt sich um Denkansätze, die mit breitem Interpretationsspielraum jeweils auf die spezifischen Gegebenheiten eines Unternehmens angepasst werden müssen. Betriebe mit umfassenden Gefährdungen im Vermögensbereich werden hier aus nachvollziehbaren Gründen zu anderen Schlussfolgerungen finden, als solche, für die entsprechende Risiken weniger bestimmend sind.

- Generelle Maßnahmen und Randbedingungen

Da die Nutzungsoptionen von Prüfsoftware ein weites Spektrum, beginnend bei der unkritischen Zusammenstellung unternehmensbezogener Informationen bis hin zur speziellen Auswertung von Personaldaten umfassen können, empfiehlt es sich, betriebliche Randbedingungen zu deren Einsatz für alle Betroffenen transparent und einvernehmlich zu formulieren. Was ist hierbei zu beachten?

- Betriebsvereinbarung

Es wird ein allseitig vermittelbares Interesse daran bestehen, dass Fehler und nachteilige Handlungen einzelner Beschäftigter nicht zu unangemessenen Risiken für das gesamte Unternehmen führen sollten. Die Fälle Siemens, Barings Bank, Société Générale sowie zuletzt UBS, die teilweise Schäden in Milliardenhöhe nach sich gezogen haben, weisen in diese Richtung. Soweit computergestützte Prüfungstechniken in diesem Zusammenhang ein geeignetes, wirtschaftliches und angemessenes Hilfsmittel zur Risikominderung darstellen, sollte innerhalb einer Betriebsvereinbarung ein Ausgleich gefunden werden, zwischen diesem gemeinsamen Interesse und berechtigten Schutzwünschen der Beschäftigten. Hierzu gehört eine Zweckbindung des Einsatzes von Prüfsoftware. Was ist das konkrete Einsatzspektrum, auf das sich alle Beteiligten einigen können? Individuelle Leistungskontrollen gehören hierbei sicherlich weder zu den Revisionsaufgaben, noch sollten sie sich auf den Einsatz dieser Programme stützen.

Mit Blick auf die neue Gesetzeslage sollten darüber hinaus Anonymisierungs- oder Pseudonymisierungsvorgänge einschließlich der hiervon betroffenen Daten behandelt werden.

Weitere Regelungsbereiche betreffen die Mitwirkung des Betriebsrates sowie des Datenschutzbeauftragten, sobald im Verdachtsfall mit konkreten Personaldaten gearbeitet werden muss. Zuletzt gilt es auf die gesetzlich vorgegebenen Rechte betroffener Arbeitnehmer (Informationslöschung) sowie Speicher- und Löschrufen einzugehen.

- Arbeitsvertragliche Regelungen

Es dürfen weder durch eine Betriebsvereinbarung noch durch einzelvertragliche Regelungen die Zwecke der aufgeführten Datenschutzbestimmungen nachteilig abgewandelt werden. Da in der Literatur unterschiedliche Ansichten darüber bestehen, ob die Regelungen innerhalb einer Betriebsvereinbarung ausreichend sind, um in konkreten Verdachtsfällen Analysen zu mitarbeiterbezogenen Daten vornehmen zu können, empfehlen sich ergänzend einzelvertragliche Regelungen mit den Mitarbeitern anzustreben.

- Beispiele und Ablaufbeschreibungen

Über die formalen Aspekte hinaus sollten revisionsbezogene Auswertungsverfahren in Beispielen kategorisiert und eingeordnet werden.<sup>1</sup>

Analyseobjekte	Erläuterungen/Betrachtungsobjekt	Voraussetzungen
Einkauf (Waren und Dienstleistungen)	Einhaltung der vorgeschriebener Prozesse	
Lagerhaltung	Ordnungsmäßige Inventur / Bestandsführung	
Zahlungsverkehr	Ordnungsmäßige Abwicklung der Überweisungen	
Kreditoren-/ Debitorenbuchhaltung	Ordnungsmäßige Abbildung der Geschäftsvorfälle	
Lohn- und Gehaltsabrechnung	Ordnungsmäßige Abrechnung	
Vertrieb	Ordnungsmäßige Provisionierung und Rabattierung	
Logistik/Fracht	Ordnungsmäßige Abrechnung	
Reisekosten	Richtlinieneinhaltung und Ordnungsmäßigkeit	
Zahlungsverkehr	Anonymisierter Datenabgleich mit Kontenverbindungen von Beschäftigten.	Generelle Abstimmung des Vorgehens mit der Personalvertretung und dem Datenschutzbeauftragten
Zahlungsverkehr	Konkrete Zusammenstellung geschäftlicher Zahlungsverkehrsdaten einzelner ausgewählter Beschäftigter	Einzelabstimmung mit der Personalvertretung und dem Datenschutzbeauftragten

- Anonymisierung / Pseudonymisierung

Zu generell vorbereitenden Maßnahmen zählt weiterhin die Festlegung, nach welchen Kriterien und mit welchen Verfahren Anonymisierungen bzw. Pseudonymisierungen personenbezogener Daten erfolgen. Einige speziell auf Revisionssoftware zugeschnittene Transferprogramme werben mit Verschlüsselungsmöglichkeiten bereits während der Datenübertragung. Es sollte darüber hinaus eine der wesentlichen *Anforderungen an die Hersteller und Verreiber von Prüfsoftware* sein, den gesetzlichen Bestimmungen entsprechende, nachvollziehbare Pseudonymisierungsmöglichkeiten für kritische Datenfelder standardmäßig als Programmfunktion bereitzustellen. Hierauf gerichtete Entwicklungen dürften sich für die Verbreitung dieser Programme zukünftig sicherlich als nützlicher erweisen, als die „automatisierte“ Auswertung undifferenzierter Massendaten.

- Dokumentationsverfahren

Transparenz und Nachvollziehbarkeit sind wesentliche Anker für Compliance-gerechte Datenanalysen. Die hierfür innerhalb der Software zur Verfügung stehenden „Audit-Trails“ sind hierfür nur bedingt (IDEA) oder überhaupt nicht (ACL) geeignet. Hier bedarf es insbesondere bei der Analyse kritischer personenbezogener Daten ergänzend eines festgelegten manuellen Aufzeichnungsverfahrens, welches sich z.B. mit vorbereiteten Formularen an der Arbeitspapiertechnik externer Wirtschaftsprüfer orientiert.

<sup>1</sup> In Anlehnung an GDD / DIIR Ausarbeitung „Datenauswertungen und personenbezogene Datenanalyse“, Beispiele für den praktischen Umgang im Revisionsumfeld

- Vorgehen bei verdachtsabhängigen Analysen und personenbezogenen Daten

Soweit sich über die generellen Vorbereitungen hinaus in Verdachtsfällen die Notwendigkeit ergibt, mit mitarbeiterbezogenen Daten zu arbeiten, empfiehlt sich ebenfalls ein nachvollziehbares Vorgehen in einzelnen festgelegten Schritten:

- Definition und Abgrenzung prüferischer Fragestellungen einschließlich der hiermit verbundenen mitarbeiterbezogenen Daten
- Informationen und Abstimmungen mit der Personalvertretung sowie gegebenenfalls dem Datenschutzbeauftragten entsprechend dem in der Betriebsvereinbarung festgelegten Eskalationsverfahren
- Aktivierung des besonderen Dokumentationsverfahrens
- Beurteilung verdachtsabhängiger Ergebnisse und schließlich deren Sicherung, soweit die Datenbestände den Verdacht erhärten
- Löschung von Daten, soweit sich der Verdacht nicht bestätigt hat und nachfolgende Information des Betroffenen

## **7 Schlussfolgerung**

Die in der Vergangenheit kontrovers und öffentlichkeitswirksam diskutierten „Datenskandale“ können bei einer differenzierten Datenbetrachtung nur begrenzt mit digitalen Auswertungstechniken der Internen Revision in Verbindung gebracht werden. Gleichwohl waren die betrieblichen Revisionsstellen durch die starke Entwicklung hin zu automatisierten Massendatenanalysen einschließlich der hiermit verbundenen nachteiligen Begrifflichkeiten nicht ganz unbeteiligt an den Irritationen, die sowohl in der Öffentlichkeit als auch der Arbeitnehmerschaft, den Personalvertretungen sowie Datenschutzbeauftragten entstanden sind.

Der Gesetzgeber hat hierauf mit Vorschriften reagiert, die nachfolgend praktischen Erfordernissen angepasst werden. Hiervon sind insbesondere die über die digitale Datenanalyse hinausgehenden forensischen Untersuchungen (Videoüberwachung, Analyse von E-Mail und Internet-Nutzung, Einsatz von Biometrieverfahren etc.) betroffen. Bezogen auf den engeren Bereich der revisionsbezogenen Auswertung von Geschäftsdaten erweisen sich die vorgesehenen Rahmenbedingungen hingegen als überschaubar. In der Verantwortung des Managements liegende Leistungs- und Verhaltenskontrolle auf der Grundlage reiner Geschäftsdaten bleibt erlaubt. Die in der öffentlichen Diskussion inkriminierten Abgleiche mitarbeiterbezogener Daten sind weiterhin möglich, wenn sie begründbar, angemessen, transparent und unter dem zusätzlichen Einsatz von Anonymisierungs- / Pseudonymisierungstechniken durchgeführt werden. Dies war bereits in der Vergangenheit in vielen Revisionsabteilungen der Fall. Bei konkreten Untersuchungen in Verdachtsfällen unter Einbeziehung nichtanonymisierter Mitarbeiterdaten sind mit Mitwirkungs- und Informationspflichten von Datenschutzbeauftragten sowie der Personalvertretung zu beachten. Dieses dürfte – bei Licht betrachtet – auch keine wesentliche Änderung gegenüber früheren Handhabungen darstellen.

Mit Bezug auf die erweiterten Bestimmungen des Bundesdatenschutzgesetzes sollten Betriebsvereinbarungen und verbindliche Vorgehensmodelle entwickelt werden, um weitere nachteilige, häufig unbegründete öffentliche oder betriebliche Diskussionen zukünftig zu vermeiden.