

Korruptionsverhinderung und Datenschutz – die Sicht der Internen Revision

BDA Symposium Arbeitnehmerdatenschutz
Berlin, 28. Juni 2011

Volker Hampel
DIIR – Deutsches Institut für Interne Revision e.V.

Inhalte

- ▶ Das DIIR – Deutsches Institut für Interne Revision e.V.
- ▶ Ansatz: Haftung der Unternehmensleitung
- ▶ Datenanalysen – Problembereiche
- ▶ Datenanalysen – Lösungsansätze

Inhalte

- ▶ Das DIIR – Deutsches Institut für Interne Revision e.V.
- ▶ Ansatz: Haftung der Unternehmensleitung
- ▶ Datenanalysen – Problembereiche
- ▶ Datenanalysen – Lösungsansätze

Das DIIR versteht sich als berufsständische Vertretung der Internen Revisoren mit derzeit ca. 2.400 Mitgliedern aus vielen Branchen.



Inhalte

- ▶ Das DIIR – Deutsches Institut für Interne Revision e.V.
- ▶ Ansatz: Haftung der Unternehmensleitung
- ▶ Datenanalysen – Problembereiche
- ▶ Datenanalysen – Lösungsansätze

- ▷ Relevante Termini: **Sorgfaltspflicht** und Organhaftung; „ordentlicher Geschäftsleiter“
- ▷ Haftung: bei vorsätzlichem oder fahrlässigem **Unterlassen** (auch bezüglich **Kontrollmaßnahmen**)
- ▷ §§ 93 (2) AktG, § 43 GmbHG, § 130 OWiG: **Schadensersatzpflicht** bei **Pflichtverletzungen**
- ▷ Bsp. **Pflichtverletzung**: Unterlassung von Aufsichtsmaßnahmen, um Zuwiderhandlungen gegen Pflichten zu verhindern oder zu erschweren (§ 130 OWiG)

Wie können Aufsichtspflichten exemplarisch definiert werden?

Institut der Wirtschaftsprüfer (IDW):

IDW PS (Prüfungsstandard) 261: „Internes Kontrollsystem“:

- ▷ Dient zur Sicherung der **Wirksamkeit** und **Wirtschaftlichkeit** der **Geschäftstätigkeit** inklusive **Vermögensschutz**
- ▷ Begreift auch ein: die **Verhinderung** und **Aufdeckung** von **Vermögensschädigungen**

Bilanzrechtsmodernisierungsgesetz (BilMoG): wichtiger Kommentar zu § 107 AktG aus dem Regierungsentwurf

- ▷ Der Aufsichtsrat sollte eigene Sorgfaltspflichtverletzungen ausschließen, indem er den Vorstand veranlasst, stringente Kontrollsysteme und Informationsabläufe zu installieren.

Inhalte

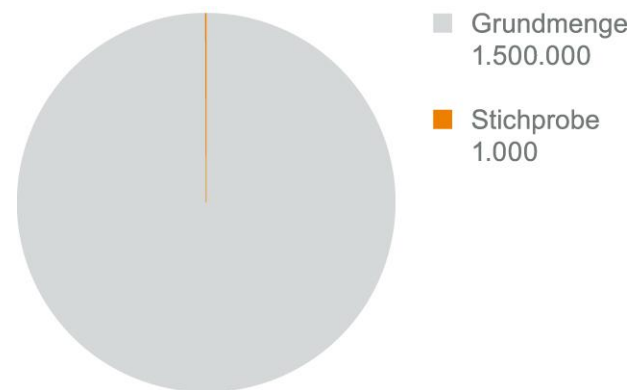
- ▶ Das DIIR – Deutsches Institut für Interne Revision e.V.
- ▶ Ansatz: Haftung der Unternehmensleitung
- ▶ Datenanalysen – Problembereiche
- ▶ Datenanalysen – Lösungsansätze

Datenanalysen – Problembereiche

- ▶ Interne Kontrollen und Internes Kontrollsystem müssen mit dem technischen Wandel (IT) Schritt halten. Datenanalysen erlauben das Auffinden von „red flags“ (Doppelbuchungen, Mehrfachrechnungen etc.) in umfangreichen Datenbeständen.
- ▶ IT-gestützte Methoden/Instrumente sind dabei für die Prävention wirtschaftskrimineller Handlungen unentbehrlich, um eine effektive Chance auf das Erkennen wirtschaftskrimineller Handlungen zu haben.

Praktisches Beispiel eines deutschen Großunternehmens

- ▶ Im 125. Jahr des Bestehens wickelt die Bosch-Gruppe für das Inlandsgeschäft und diverse angeschlossene Auslandsgesellschaften wöchentlich im Schnitt ca. 30.000 ausgehende Zahlungen (Zahlungstransaktionen, „Commercial Payments“, also keine Gehaltszahlungen o.ä.) ab.
 - ▶ Auf das gesamte Jahr hochgerechnet sind dies ca. 1,5 Millionen.
 - ▶ Wer soll solch ein Volumen – selbst stichprobenweise – kontrollieren?
- ▶ Fiktives Beispiel: „Menschlicher“ Revisor zieht bei zweimal p. a. stattfindender Prüfung im Zahlungsverkehr physische Stichprobe von jeweils 500 Zahlungsbelegen (Summe = 1000; entsprechend 0,067 % der Grundmenge).

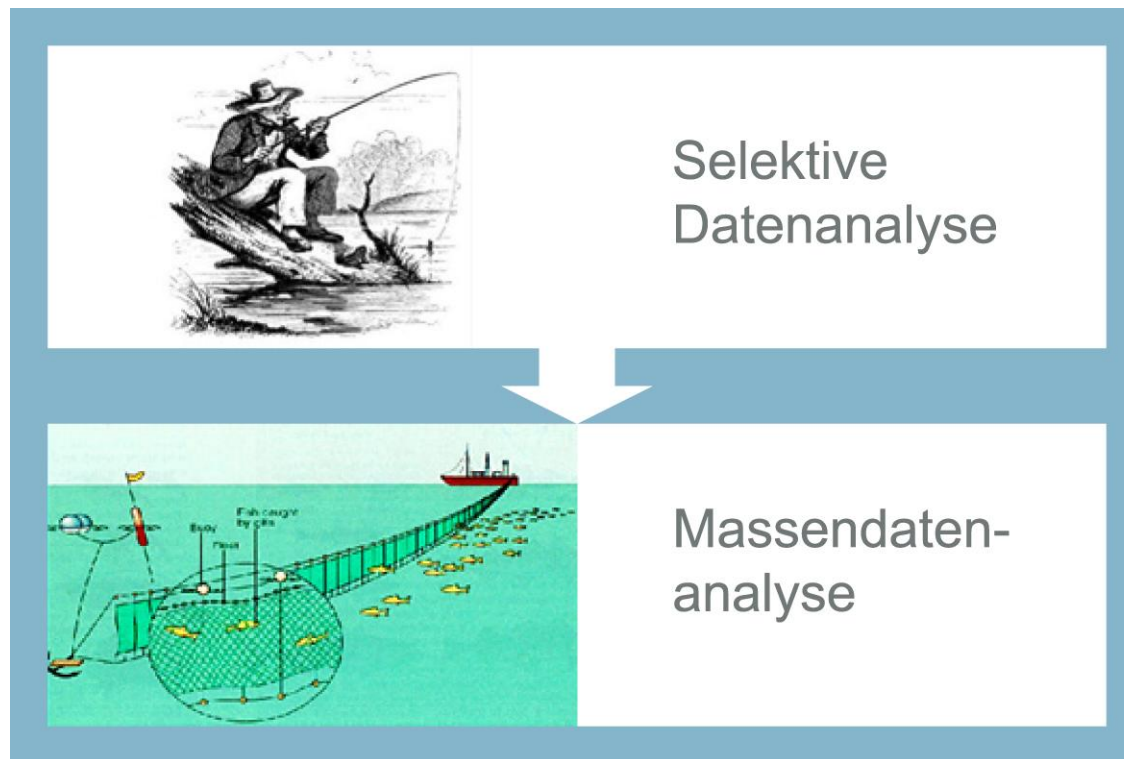


Datenanalyse-Problem: Logisch separierte Datenbestände wurden zusammengeführt (es geht auch anders!)



Datenanalyse ≠ personenbezogene Daten!

Das Grundproblem muss gelöst werden – selektive vs. Massendatenanalyse



Quelle: DIIR und GDD – Datenauswertungen und personenbezogene Datenanalysen, S. 8, Frankfurt 2009

Inhalte

- ▶ Das DIIR – Deutsches Institut für Interne Revision e.V.
- ▶ Ansatz: Haftung der Unternehmensleitung
- ▶ Datenanalysen – Problembereiche
- ▶ Datenanalysen – Lösungsansätze

Exemplarisch: Beschluss des Bundesverfassungsgerichts vom 17. Februar 2009

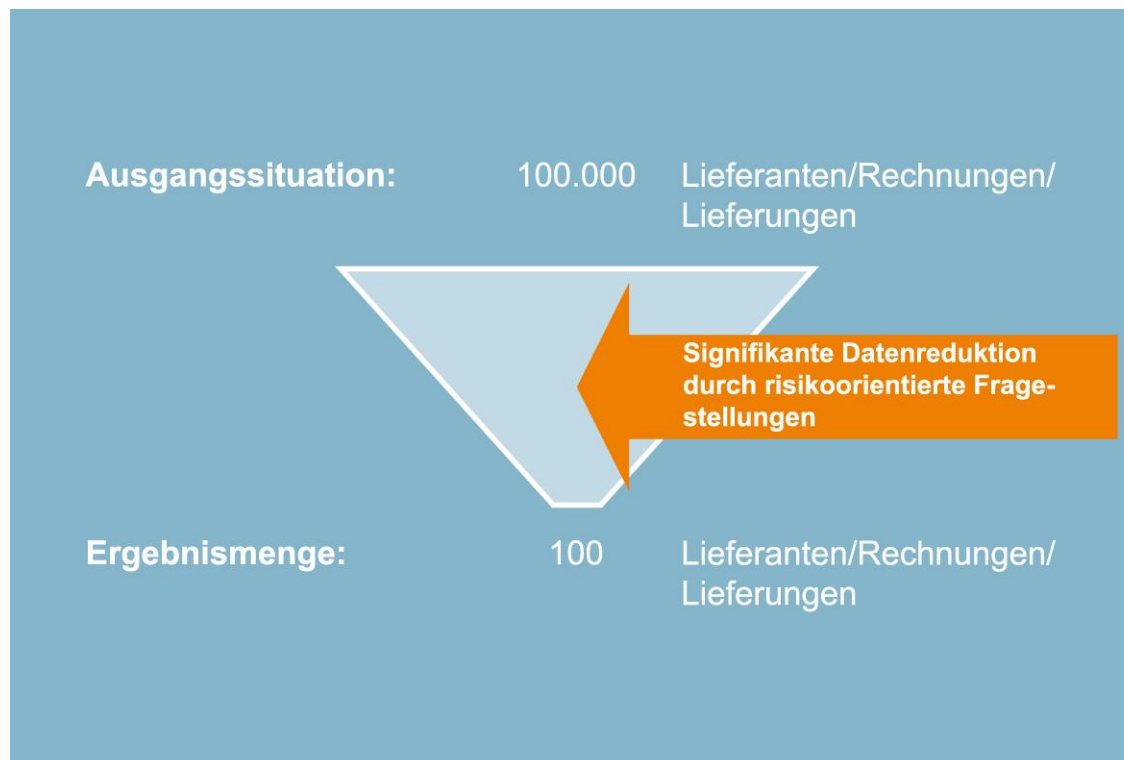
(BVerfG, 2 BvR 1372/07 vom 17.2.2009, Absatz Nr. 19)

- ▷ Die maschinelle Überprüfung von Überweisungsdaten stellt keine Verletzung des informationellen Selbstbestimmungsrechts Betroffener dar, wenn die nicht potenziell Tatverdächtigen im Rahmen der Analyse anonym und spurlos beim eigentlichen „Suchlauf“ extrahiert werden.
- ▷ Bsp.: Mehrere Millionen Kreditkartenumsätze anhand dreier definierter Kriterien (Betrag, Empfänger, Zeitraum) durchsucht.
- ▷ Im Ergebnis final 322 Datensätze extrahiert, d. h. mehrere Millionen Datensätze wurden „überlesen“ oder im Wortlaut des Bundesverfassungsgerichts „spurlos aus dem Suchlauf ausgeschieden“.

Datenanalysen: Lösungsansätze

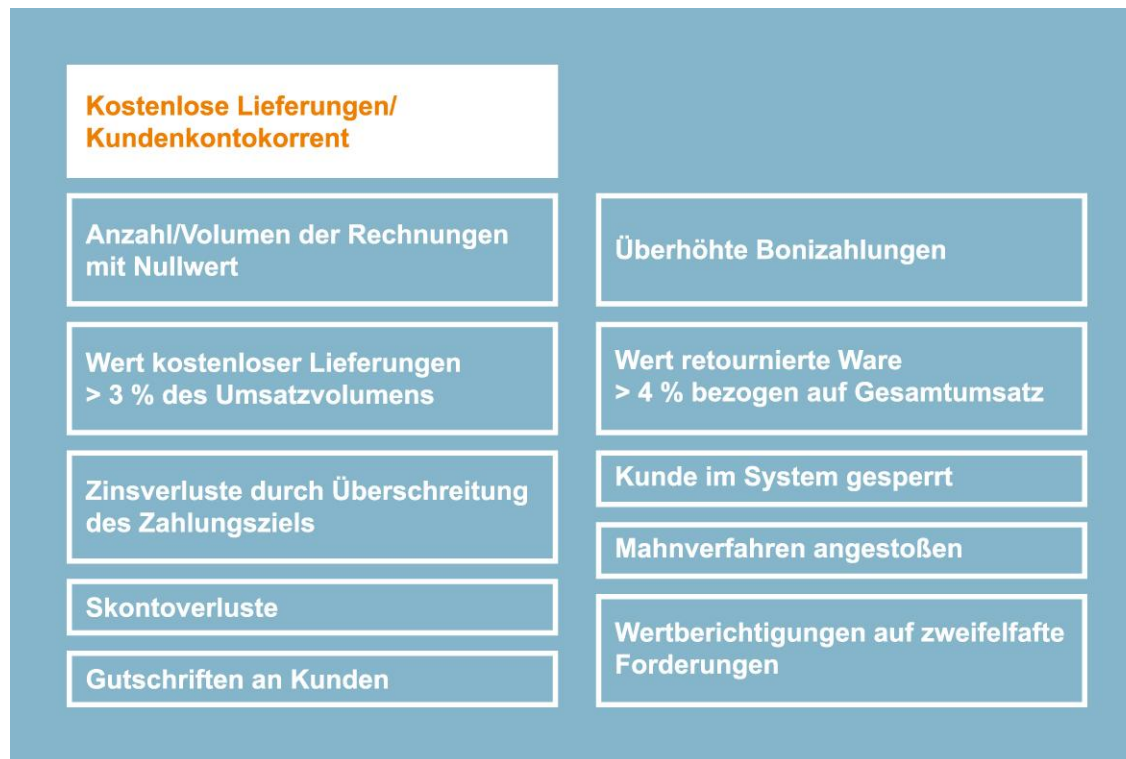
- ▶ Notwendige Analysen sind in aller Regel auf Geschäftsdatenbasis (losgelöst von personenbezogenen Daten) durchzuführen.
- ▶ Mit entsprechender Vorbereitung und Anonymisierung können „Verdachtsfälle“ identifiziert werden.
- ▶ Viele Analysen erfordern erst am Ende des Analyseprozesses, einen Bezug zu Personen herzustellen.
- ▶ Dies kann dann auf der Basis der manifestierten Indizien passieren.
- ▶ Wichtig ist ein geplantes, strukturiertes Vorgehen.

Beispiel: Identifikation illegitimer kostenloser Lieferungen



Quelle: DIIR und GDD – Datenauswertungen und personenbezogene Datenanalysen, S. 35, Frankfurt 2009

Beispiel: Identifikation illegitimer kostenloser Lieferungen



Quelle: DIIR und GDD – Datenauswertungen und personenbezogene Datenanalysen, S. 34, Frankfurt 2009

Beispiel: Identifikation illegitimer kostenloser Lieferungen

Lieferanten-Nr.	Frage										Total
	1	2	3	4	5	6	7	8	9	10	
7008765	1	1	0	1	1	1	1	1	1	0	8
7006754	1	1	1	0	1	0	1	0	1	1	7
7006548	1	1	1	1	0	1	1	0	1	0	7
7005465	1	1	1	0	1	1	0	0	0	0	5
7006547	1	1	0	0	1	0	1	0	1	0	5
7003254	1	0	0	1	1	0	1	0	1	0	5
7007865	1	1	0	0	1	1	0	0	0	0	4
7009876	1	1	0	0	0	0	1	0	1	0	4
7005439	1	1	1	0	0	0	0	0	1	0	4
7004357	1	0	0	0	0	0	1	0	1	0	3

Quelle: DIIR und GDD – Datenauswertungen und personenbezogene Datenanalysen, S. 35, Frankfurt 2009

Lösungsvorschlag DIIR/GDD* – auch anwendbar bei aktueller Fassung des § 32 BDSG –

Prozessunabhängig

Abfassung einer Verfahrensanweisung oder Betriebsvereinbarung zum Vorgehen bei personenbezogenen Datenanalysen; Beispiele für Inhalt:

- ▷ Prüfungstätigkeit der Internen Revision erfordert nicht die Abstimmung mit BR und/oder DSB.
- ▷ Für reguläre Revisionsarbeit sind automatisierte Analysen notwendig; sie werden mit der Verfahrensanweisung als zulässiges Instrument freigegeben.
- ▷ Erst weiterführende personenbezogene Analysen erfordern Einbindung BR und DSB.

* DIIR und GDD – Datenauswertungen und personenbezogene Datenanalysen, Frankfurt 2009

Lösungsvorschlag DIIR/GDD – auch anwendbar bei aktueller Fassung des § 32 BDSG –

Prozessabhängig

1. Untersuchungsobjekt eindeutig definieren und abgrenzen
2. Betrachtungsobjekt maximal einschränken
(minimale Verwendung personenbezogener Daten)
3. Einbezogene personenbezogene Daten anonymisieren/
pseudonymisieren
4. Beteiligte an Untersuchung einweisen
(durch Datenschutzbeauftragten)
5. Dokumentationsregeln festlegen
(idealerweise in vorgenannter Verfahrensanweisung)

Lösungsvorschlag DIIR/GDD – auch anwendbar bei aktueller Fassung des § 32 BDSG –

Prozessabhängig

6. Analysen durchführen
7. Analysen dokumentieren
(Bezug herstellen für spätere Rekonstruierbarkeit etc.)
8. Nicht risikobehaftete Daten dokumentiert unverzüglich löschen
9. Abstimmung mit eventuell einzubeziehenden Einheiten
(Recht, Personal, Betriebsrat) bei auffälligen Ergebnissen
10. Zur Einbeziehung externer Dienstleister: direkte Entnahme der
Rahmenbedingungen aus dem BDSG

Die wichtigsten Forderungen des DIIR im Gesetzgebungsverfahren zum Beschäftigten- Datenschutz

- ▶ **Korruptions- und Kriminalitätsbekämpfung erfordern automatisierte Analysen** und damit insbesondere präventive Maßnahmen. Der Arbeitnehmerdatenschutz ist zu wahren.
- ▶ Präventive Analysen dürfen **nicht an weiterführende Voraussetzungen** (bspw. des Vorliegens verdachtsbegründender Tatsachen auf eine Straftat oder schwerwiegende Pflichtverletzungen, die eine Kündigung aus wichtigem Grund rechtfertigen würden), geknüpft sein.
- ▶ Eine **Unterrichtungspflicht** an die Beschäftigten hinsichtlich der präventiven Analyse von Daten sollte **nicht** vorgegeben werden – dies hat einen Vorwarnungscharakter. Zudem motivieren erfolglose Analysen ggf. zusätzlich.

Die wichtigsten Forderungen des DIIR im Gesetzgebungsverfahren zum Beschäftigten- Datenschutz

- ▶ Die getroffenen Regelungen müssen die Möglichkeit des **Datenaustauschs zwischen Konzernunternehmen** erlauben.
- ▶ Der Abschluss von **Betriebsvereinbarungen** zum Arbeitnehmerdatenschutz muss unverändert für die Erhebung, Nutzung und Verarbeitung von Daten zulässig sein, um **betriebsnahe Lösungen** zu ermöglichen.
- ▶ **Unbestimmte Begrifflichkeiten** wie „Erforderlichkeit“ sollten nicht zum Maßstab für die Zulässigkeit von Datenanalysen gemacht werden – hier sind vielmehr weiterführende Definitionen sinnvoll. So könnten **Geschäftsdaten** als „...überwiegend dem Geschäftsbetrieb des Arbeitgebers...“ zuzurechnende Daten definiert werden.