

# Inhaltsverzeichnis

Vorwort .....	5
Inhaltsverzeichnis .....	7

Prof. Dr. Norbert Nolte

## **Datenanalyse und Datenschutz - Leitlinien für die interne Revision** ..... 11

1 Einführung .....	13
2 Der Beschäftigtendatenschutz als Grenze der Revisionstätigkeit (§32 BDSG) .....	15
2.1 Verfassungsrechtlicher Hintergrund .....	15
2.2 Datenschutzrechtlicher Hintergrund .....	15
2.2.1 Einwilligung im Beschäftigtendatenschutz .....	15
2.2.2 Betriebsvereinbarungen regelmäßig keine taugliche Alternative .....	16
2.2.3 Anwendungsbereich des §32 BDSG .....	17
2.2.4 Rechtfertigung der Datenanalyse durch §32 BDSG .....	19
2.2.4.1 Präventive Maßnahmen .....	20
2.2.4.2 Repressive Maßnahmen .....	22
2.2.5 Datenabgleiche .....	23
3 Grenzen der Revisionstätigkeit durch das Fernmeldegeheimnis .....	27
3.1 Der Arbeitgeber als TK-Anbieter .....	27
3.2 Reichweite des Fernmeldegeheimnisses .....	28
3.3 Mitteilung an andere Personen .....	29
3.4 Unbefugt .....	29
3.5 Zusätzlich: Datenschutzrecht anwendbar .....	30
4 Auftragsdatenverarbeitung .....	31
5 Zusammenfassung .....	32

Anke Giegandt

## **Datenschutz bei der Analyse von Massendaten in Revisionsprozessen** ..... 33

1 Ausgangssituation .....	35
2 Rahmenbedingungen .....	36
2.1 Begriffsbestimmungen .....	36
2.2 Aufgaben der Internen Revision .....	36
2.3 Unterscheidung Standard-Revision und Sonderuntersuchung .....	37
2.4 Relevante Gesetze – Gesetzliche Regelungen zum Schutz des Unternehmens .....	38
2.5 Relevante Gesetze – Betriebsverfassungsgesetz (BetrVG), Bundesdatenschutzgesetz (BDSG) und EU-Datenschutzrichtlinie .....	38
2.5.1 Bundesdatenschutzgesetz (BDSG) .....	39
3 Datenschutzkonzept bei Datenanalysen der Internen Revision .....	40

4	Fallbeispiele und Zusammenfassung .....	43
4.1	Analyseergebnisse mit und ohne Pseudonymisierung.....	43
4.1.1	Vergleich Benutzer und Lieferant .....	43
4.1.2	Prüfung der Einhaltung von BSH-internen Regelungen im Einkaufsprozess .....	44
4.1.3	Prüfung auf Missbrauch im Einkaufsprozess (Rechnungsbetrag vs. Bestellbetrag).....	45
4.1.4	Prüfung auf Missbrauch im Einkaufsprozess (Ersteller der Lieferanten-Grunddaten vs. Bestellerfasser vs. Freigeber der Bestellung).....	47
4.1.5	Prüfung auf Doppelzahlungen an Lieferanten.....	47
4.1.6	Analyse von Berechtigungen in IT-Systemen .....	48
4.2	Zusammenfassung .....	49
5	Quellenangaben.....	49
6	Abkürzungerverzeichnis .....	50

Dipl.-Volkswirtin Evelyn Schmidt

## **Korruptionsverhinderung und Datenschutz – Die Sicht der Internen**

	Revision .....	51
1	Einleitung .....	53
2	Das DIIR – Deutsches Institut für Interne Revision e.V. .....	54
3	Die Haftung der Unternehmensleitung .....	54
4	Rolle der Internen Revision bei der Unternehmensüberwachung .....	56
5	Begriffliche Abgrenzungen.....	56
6	Problembereich von Datenanalysen.....	58
7	Datenanalysen: Lösungsansätze.....	60
7.1	Das Vorgehen bei einer Datenanalyse am Beispiel der „Identifikation illegitimer kostenloser Lieferungen“ .....	61
8	Lösungsvorschlag DIIR/GDD .....	66
8.1	Prozessunabhängige Handlungsempfehlungen .....	66
8.2	Prozessabhängige Handlungsempfehlungen (d.h. die Prüfung von Daten mit Personenbezug) .....	66
9	Die wichtigsten Forderungen des DIIR im Gesetzgebungsverfahren zum Beschäftigten-Datenschutz.....	68

Prof. Dr. Georg Herde / Prof. Andreas Kohl

	Umfrage zur Akzeptanz der Digitalen Prüfungsunterstützung .....	69
1	Zusammenfassung.....	71
2	Ausgangssituation und Fragestellung .....	71
3	Zur Methode und zum Stand der Untersuchung .....	72
4	Beschreibung der Stichprobe .....	73
5	Ausgewählte Ergebnisse .....	75
6	Diskussion .....	82

7	Quellen .....	83
Prof. Dr. Georg Herde / Ernst Rudolf Töller		
<b>Zukunftsorientierte Analysesoftware: Anforderungen und Parameter .....</b>		85
1	Allgemeines .....	87
2	Bedeutung digitaler Datenanalyse .....	87
3	Rahmenbedingungen digitaler Datenanalyse .....	88
3.1	Unabhängigkeit von operativen Systemen .....	89
3.2	Möglichkeit der systemübergreifenden Prüfung .....	90
3.3	Standardisierte Datenformate .....	90
3.4	Verarbeitung großer Datenbestände .....	90
3.5	Benutzerfreundlichkeit der Analysesoftware .....	91
3.6	Komprimierung, Verschlüsselung und sichere Aufbewahrung .....	91
4	Methoden und Verfahren .....	92
4.1	Kennzahlen und Ratings für betriebswirtschaftliche Objekte .....	92
4.2	Umstellung von Heuristiken auf mathematische Modelle .....	93
4.2.1	Mathematisch-statistische Modelle .....	93
4.2.2	Mathematisch definierte Rankings .....	94
4.2.3	Erfolgreiche Beispiele mathematischer Modelle .....	94
5	Technische Anforderungen .....	95
5.1	Unveränderbarkeit der Daten .....	95
5.1.1	Unveränderbarkeit der Daten in den operativen Systemen .....	95
5.1.2	Unveränderbarkeit der Daten in der Analysesoftware .....	97
5.2	Nachvollziehbarkeit der Analyseschritte .....	97
5.2.1	Logging der Auswertungsschritte .....	98
5.2.2	Mehrfachverwendbarkeit von Analyseprozeduren .....	98
5.2.3	Der Schutz von Analyse Know-How .....	98
5.3	Strikte Datentypbindung .....	99
5.4	Festkommaarithmetik als Standard .....	99
5.5	Verarbeitung sehr großer Datenmengen, Desktop-/Serverversionen .....	99
6	Eigenschaften bestehender Analysesoftware .....	100
7	Literatur .....	103