Die rechtlichen Fallstricke bei der Überwachung und Durchsetzung einer Compliance-Organisation

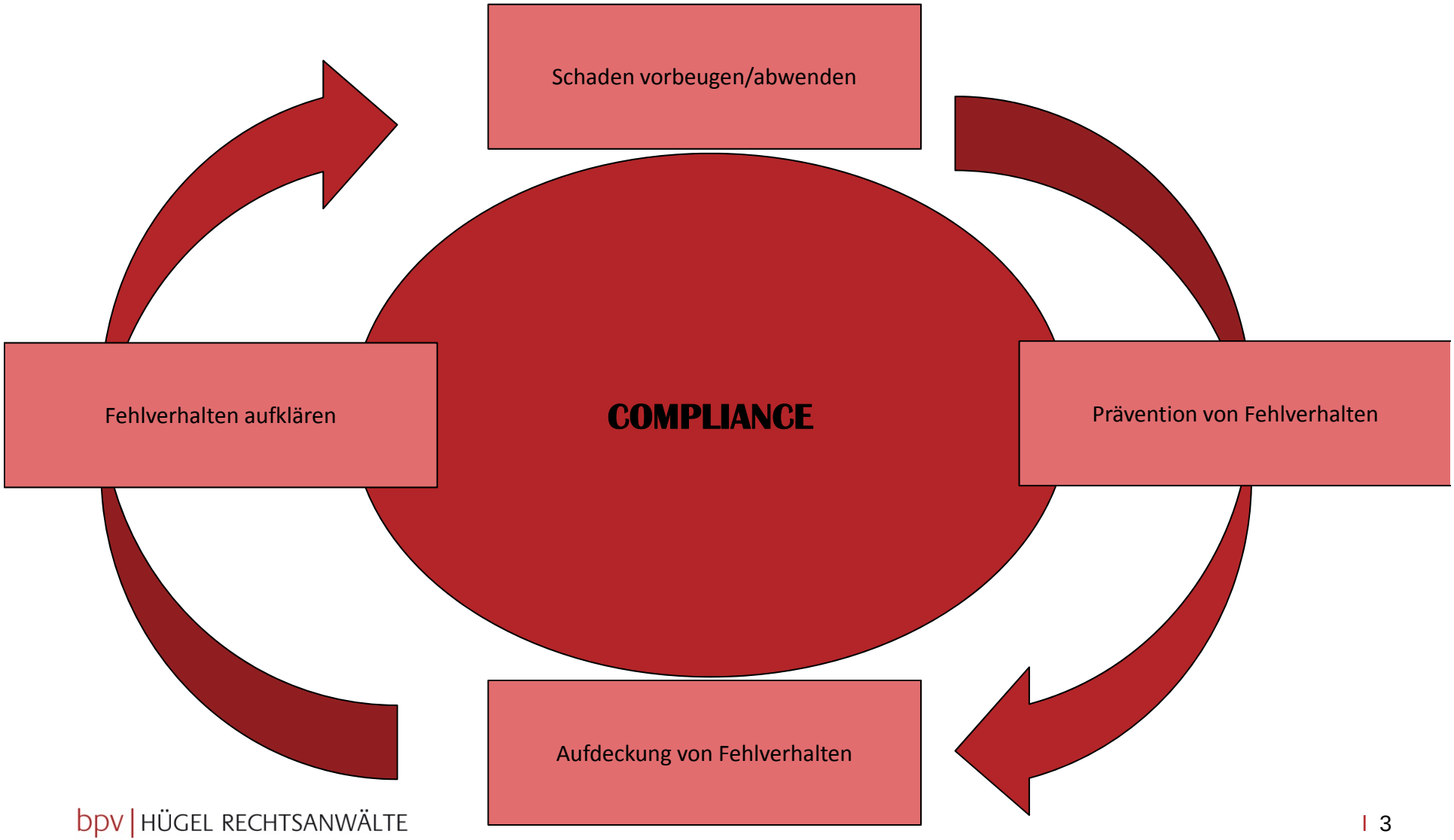
Sonja Dürager

7. Österreichischer IT-Rechtstag
Wien, 24. Mai 2013

bpv | HÜGEL RECHTSANWÄLTE

„Zauberwort Compliance“

Rechtliche Ausgangslage



Wen trifft die „Pflicht zu Compliance“?

Der Geschäftsführer muss …

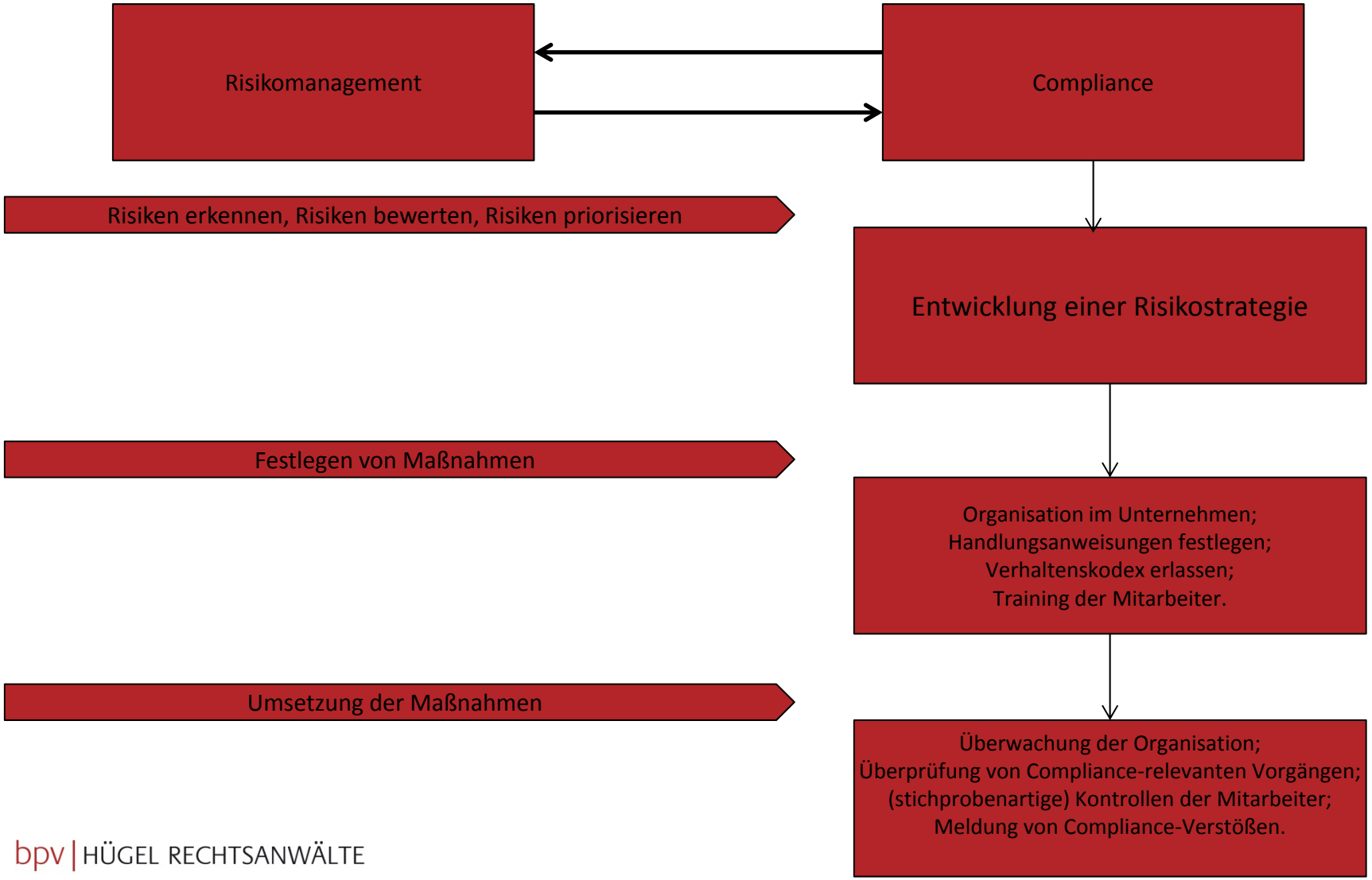
… im Rahmen der Gesetze, des Gesellschaftsvertrages und unter der gebotenen Berücksichtigung der Interessen der Öffentlichkeit und der Arbeitnehmer den Vorteil der Gesellschaft wahren und Schaden abwenden.

… das Unternehmen nach gesicherten und praktisch bewährten betriebswirtschaftlichen Grundsätzen leiten, und ein Bild von der Unternehmenslage haben.

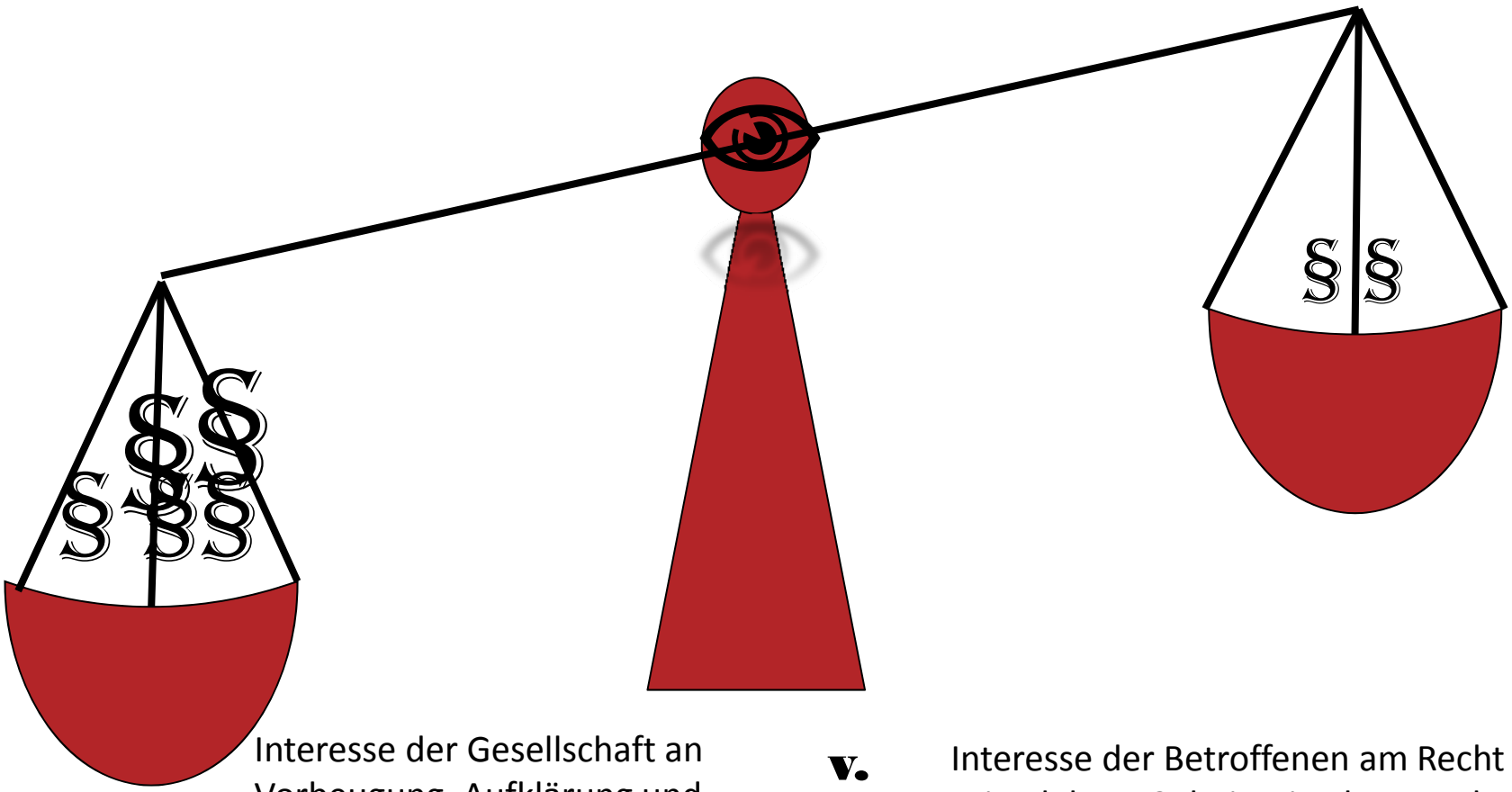
… für eine effiziente Unternehmensorganisation, welche die optimale Wahrnehmung der Aufgaben und Ziele der Gesellschaft ermöglicht, Sorgen.

… sämtliche Rechtsnormen beachten, und dafür sorgen, dass sich die Gesellschaft rechtmäßig verhält.

Ziel einer Compliance-Organisation



Data Privacy & Compliance – Das Problem ...



Interesse der Gesellschaft an Vorbeugung, Aufklärung und Verfolgung illegitimer Verhaltensweisen

v.

Interesse der Betroffenen am Recht auf Privatleben, Geheimnisschutz und informationelle Selbstbestimmung

Kontrolle der Mitarbeiter

Was wird überwacht?

- **Überwachung der Internetnutzung:**
  - ➔ Speicherung von Logfiles von Webservern
  - ➔ IP-Adresse samt angesteuerten Internetziel
  - ➔ <u>zu unterscheiden:</u>

    Aufzeichnung von systemnahen Logfiles zur Systemüberwachung

- **Überwachung der E-Mail-Kommunikation:**
  - ➔ Aufzeichnung der Verkehrsdaten (Zeitpunkt, Ziel- und Absenderadresse, Dateigröße)
  - ➔ Speicherung von Inhaltsdaten

Anwendungsbeispiel: Kontrolle nach dem BDG

5a. Unterabschnitt des BDG (§§ 79c ff BDG)

IKT: alle Einrichtungen zur elektronischen oder nachrichtentechnischen Übermittlung, Speicherung und Verarbeitung von Sprache, Text, Stand- und Bewegbildern sowie Daten

Regelung der privaten Nutzung

➔ grundsätzlich nur für dienstliche Zwecke;

➔ in einem eingeschränkten Ausmaß private Nutzung erlaubt,

- → nicht missbräuchlich ist,
- → nicht dem Ansehen des öffentlichen Dienstes schadet,
- → nicht der Aufrechterhaltung eines geordneten Dienstbetriebes entgegensteht,
- → nicht die Sicherheit und die Leistungsfähigkeit der IKT-Infrastruktur gefährdet.

Regelung der Zwecke einer Kontrolle

➔ zur Abwehr von Schäden an der IKT-Infrastruktur oder zur Gewährleistung ihrer korrekten Funktionsfähigkeit;

➔ bei einem begründeten Verdacht einer gröblichen Dienstpflichtverletzung

→ zum Zweck der Verhinderung weiterer Dienstpflichtverletzungen, wenn zeitliche, inhaltliche oder quantitative Beschränkungen der bereitgestellten IKT-Nutzung dafür nicht ausreichen

→ zum Zweck der Klarstellung des Sachverhaltes

Generelle Kriterien einer Kontrolle

Erster Schritt

- **Anonymisierte Verarbeitung**
- Verwendung statistischer Informationen
- zur Sicherstellung der Systemfunktionalität
- Kein Verdacht wegen eines Fehlverhaltens gegen eine bestimmte Person

Zweiter Schritt

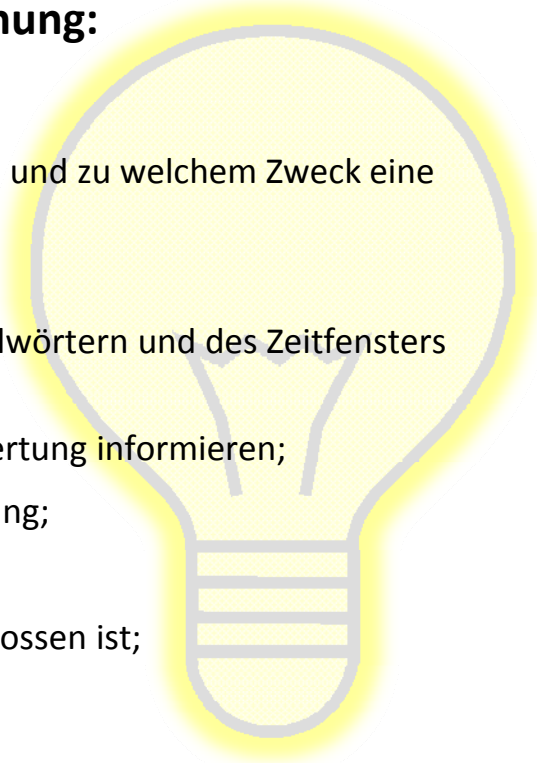
- **Pseudonymisierte Verarbeitung**
- Statistische Daten sind mit einem einer bestimmten Person zuordenbaren Code verbunden
- Vermutung eines Fehlverhaltens

Dritter Schritt

- **Identifikation des Users**
- Personenbezogene Auswertung von Verkehrs- und Inhaltsdaten
- Konkreter Verdacht gegen eine bestimmte Person

Konkrete Untersuchungshandlung

Verhältnismäßigkeit der unternehmensinternen Untersuchung:



- ➔ vorab klare Grundsätze, unter welchen Umständen und zu welchem Zweck eine Auswertung stattfinden darf;
- ➔ Definition des „konkreten Verdachts“;
- ➔ Untersuchungsauftrag (ua Festlegung von Schlüsselwörtern und des Zeitfensters für die Auswertung);
- ➔ außer bei Gefahr in Verzug Mitarbeiter über Auswertung informieren;
- ➔ Beiziehung einer Vertrauensperson zur Untersuchung;
- ➔ Dokumentation der Untersuchung;
- ➔ Löschung der Daten sobald Untersuchung abgeschlossen ist;
- ➔ **... ?**

Whistleblowing-Hotlines

Die Meldungslegung

Führung eines elektronischen Systems mit den Meldungsdaten

„Hotline“

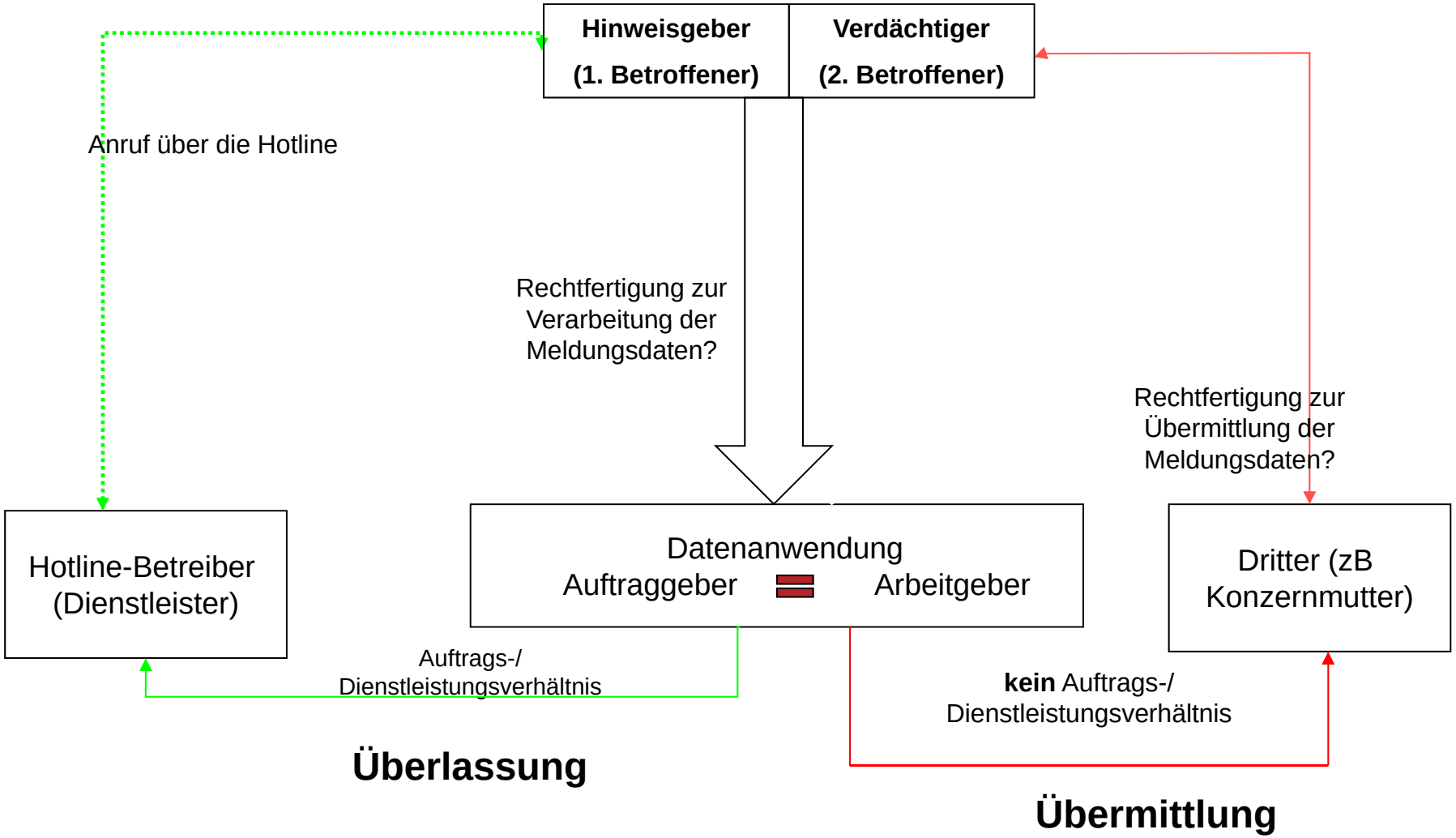
Untersuchungs- und Ermittlungsmaßnahmen?

Dienstvor-gesetzter

Verdächtiger

Whistleblower

Rollenverteilung nach dem DSG



Rechtfertigung einer Whistleblowing-Hotline

➔ **Zulässigkeit der Verarbeitung durch Arbeitgeber?**

Rechtfertigung:

- ⇨ Feststellung von rechtswidrigem Verhalten als Arbeitgeber
- ⇨ Pflicht zur Corporate Governance; Instrument einer Compliance-Organisation
- ⇨ Pflichten als Konzerngesellschaft (Über-/Unterordnung)

➔ **Zulässigkeit der Übermittlung an Konzernmutter?**

Rechtfertigung:

- ⇨ rechtliche Verpflichtungen nach SOX, dt CGK etc
- ⇨ Schutz von Konzerninteressen aber KEIN Konzernprivileg
- ⇨ Nachweis durch konzernweite Verhaltensregeln

➔ **Beachte:** Verwenden strafrechtlich relevanter Daten verlangt die Gewährleistung der Wahrung der Interessen des Betroffenen

Inhaltliche Anforderungen (I)

❶ Wieso soll der Arbeitnehmer über die Hotline melden?

☒ generelle Empfehlung des Arbeitgebers

❷ Was darf gemeldet werden?

☒ zB Straftatbestände, Rechnungslegungsvorschriften, …

explizite und taxative Aufzählung der relevanten Verstöße

❸ Wer darf gemeldet werden?

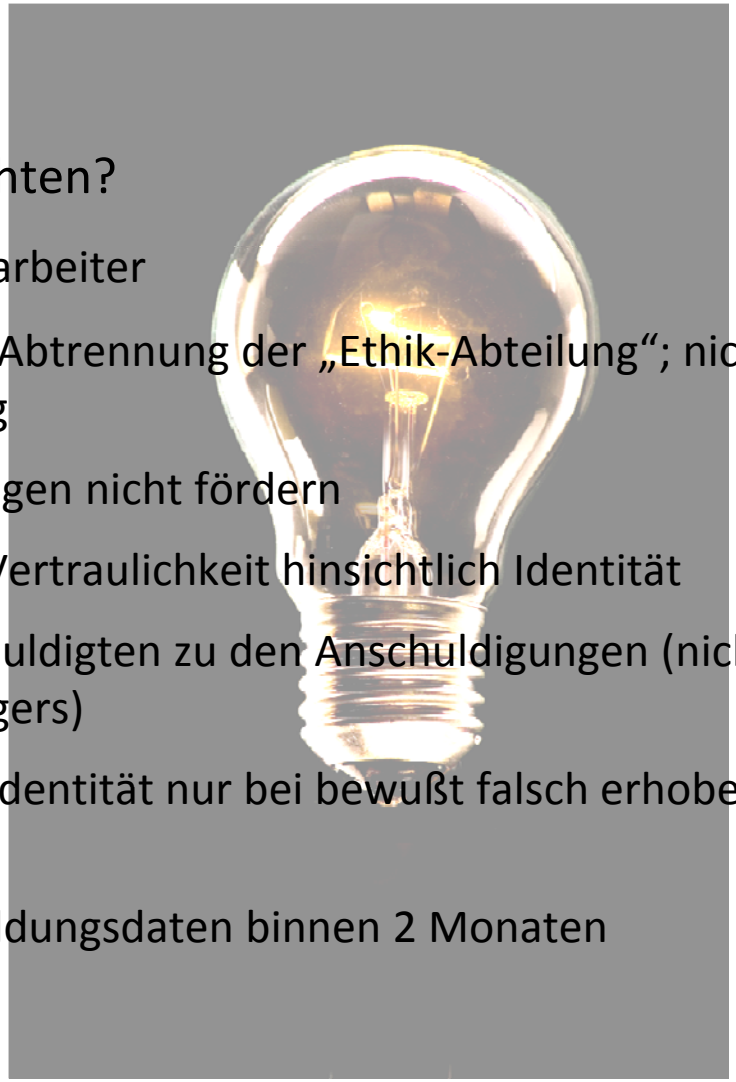
☒ Reduktion des Kreises der Betroffenen

Beachte: Weiterleitung der Meldungsdaten an Konzernmutter nur betreffend Mitarbeiter in Führungspositionen oder vergleichbar hochgestellten Positionen

Inhaltliche Anforderungen (II)

❹ Was gilt es noch zu beachten?

- ☒ Schulung der Mitarbeiter
- ☒ Organisatorische Abtrennung der „Ethik-Abteilung“; nicht Personalabteilung
- ☒ anonyme Meldungen nicht fördern
- ☒ Zusicherung der Vertraulichkeit hinsichtlich Identität
- ☒ Zugang des Beschuldigten zu den Anschuldigungen (nicht zur Person des Anzeigers)
- ☒ Offenlegung der Identität nur bei bewußt falsch erhobener Anschuldigung
- ☒ Löschung der Meldungsdaten binnen 2 Monaten



Zustimmung des Betriebsrates/Arbeitnehmers

❖ Zustimmung des Betriebsrats durch Betriebsvereinbarung

⇨ Einführung eines Kontrollmaßnahme, wenn diese die Menschenwürde berührt, aber nicht verletzt

➔ Keine Aufforderung der Mitarbeiter zur „Bespitzelung“?

⇨ wenn die Daten aus der Hotline automationsunterstützt verarbeitet werden

✋ DSK erkennt in Hinweisgebersystem ein Kontrollsystem, das *„den Mitwirkungsrechten der §§ 96, 96a ArbVG unterliegt“*.

❖ Zustimmung durch die Mitarbeiter (§ 10 AVRAG)

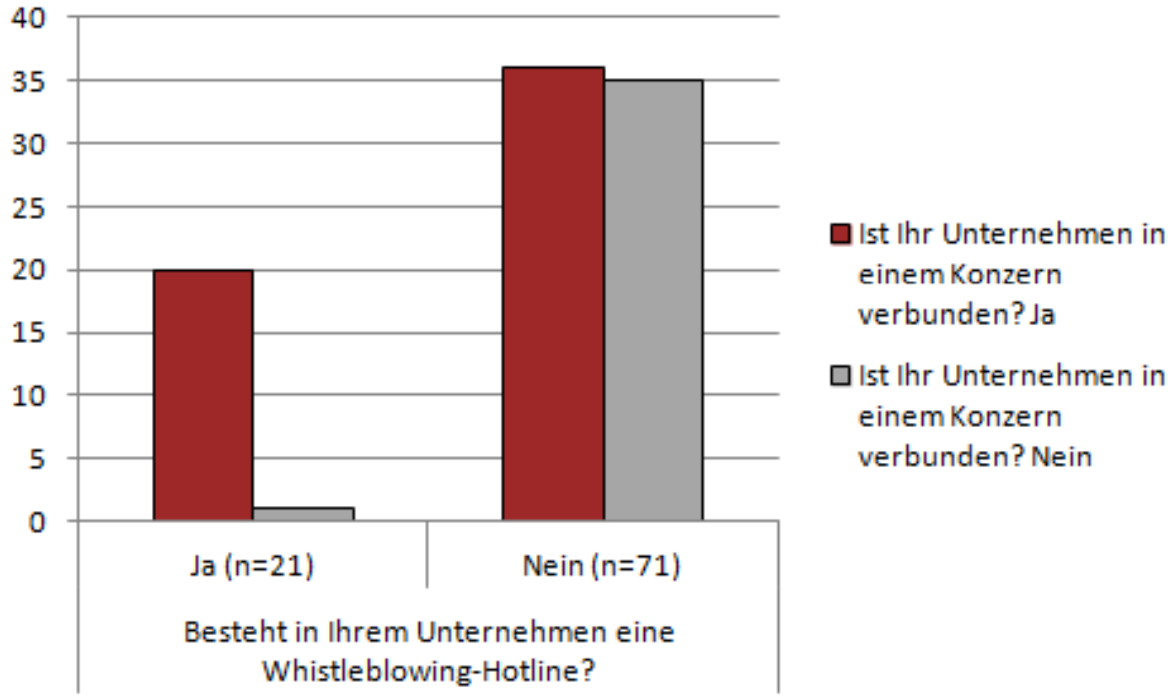
⇨ wenn kein Betriebsrat besteht und die Hotline die Menschenwürde berührt, aber nicht verletzt

Umfrage 2012

Fragestellung ...

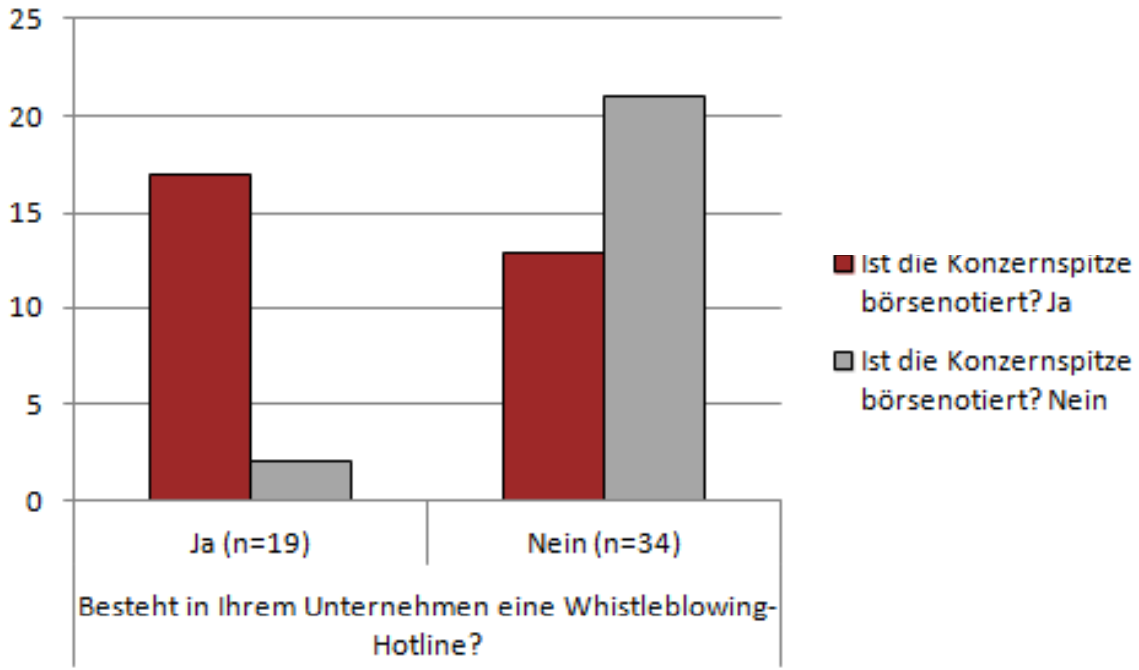
Konzernstrukturen

Die Konzernspitze muss in der Lage sein, relevante Vorgänge in den Tochtergesellschaften zu kontrollieren.



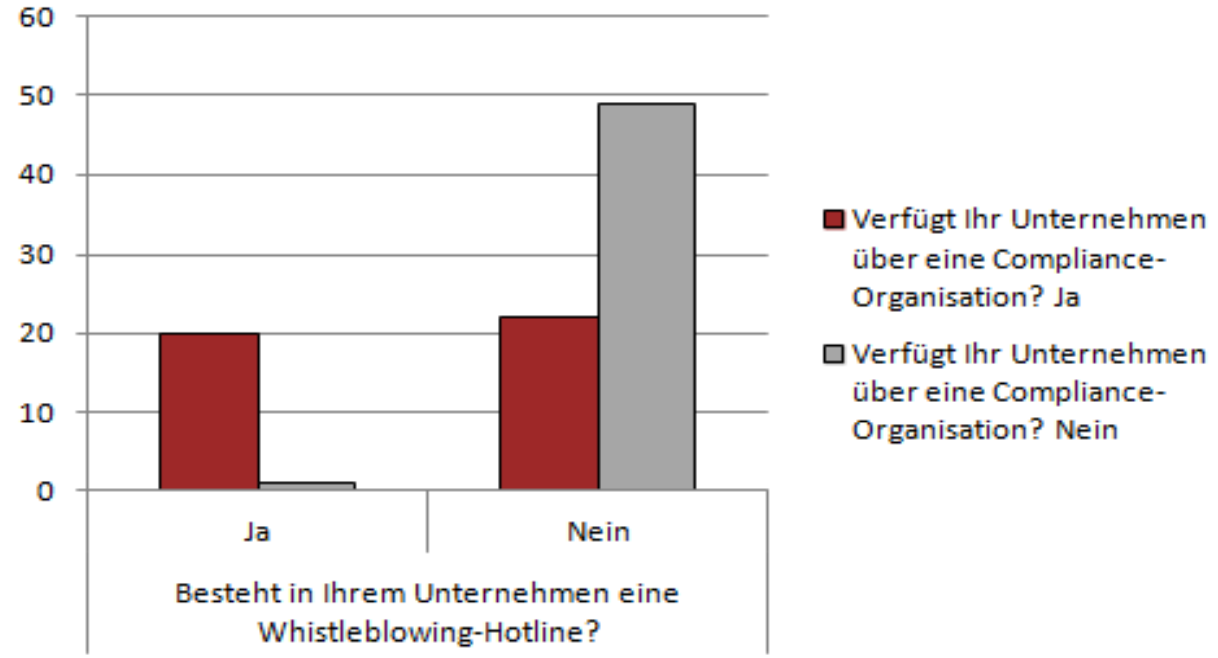
Einfluss einer Börsennotierung

Die Börsennotierung verlangt eine effektive Organisation der Corporate Compliance.



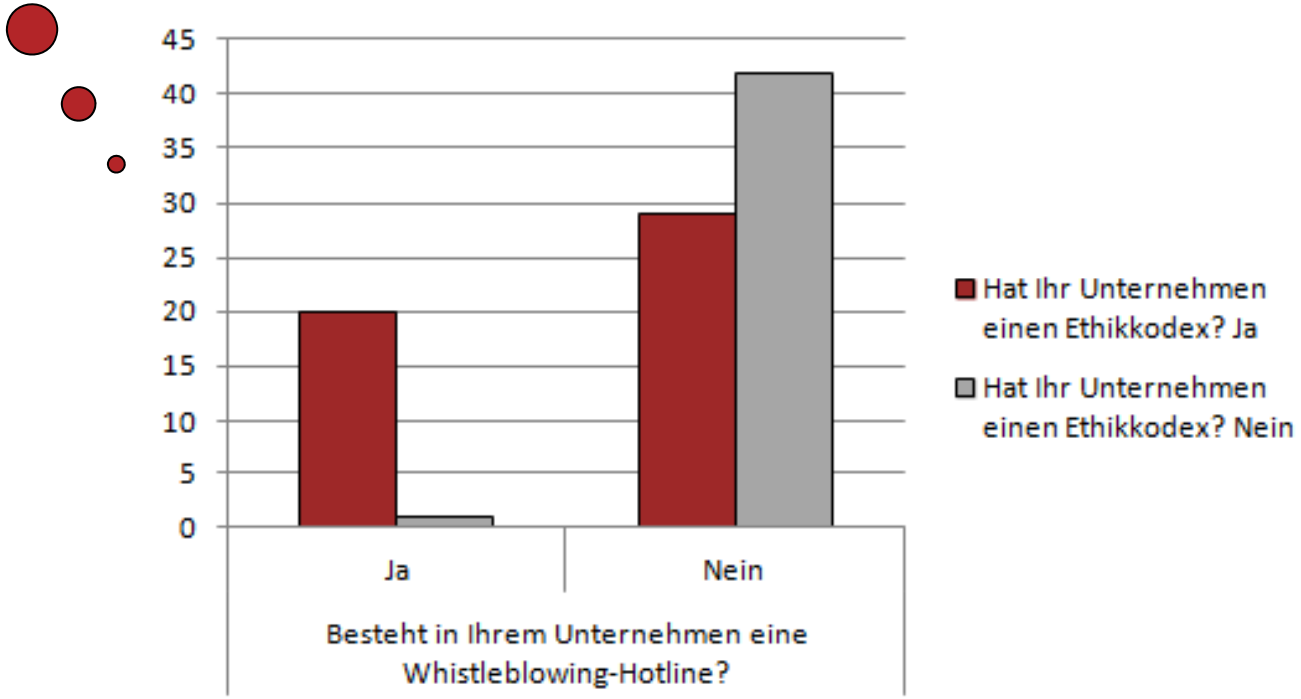
Compliance Strukturen (I)

Whistleblowing – ein wirksames Instrument einer Compliance-Organisation zur Aufdeckung von Verstößen …

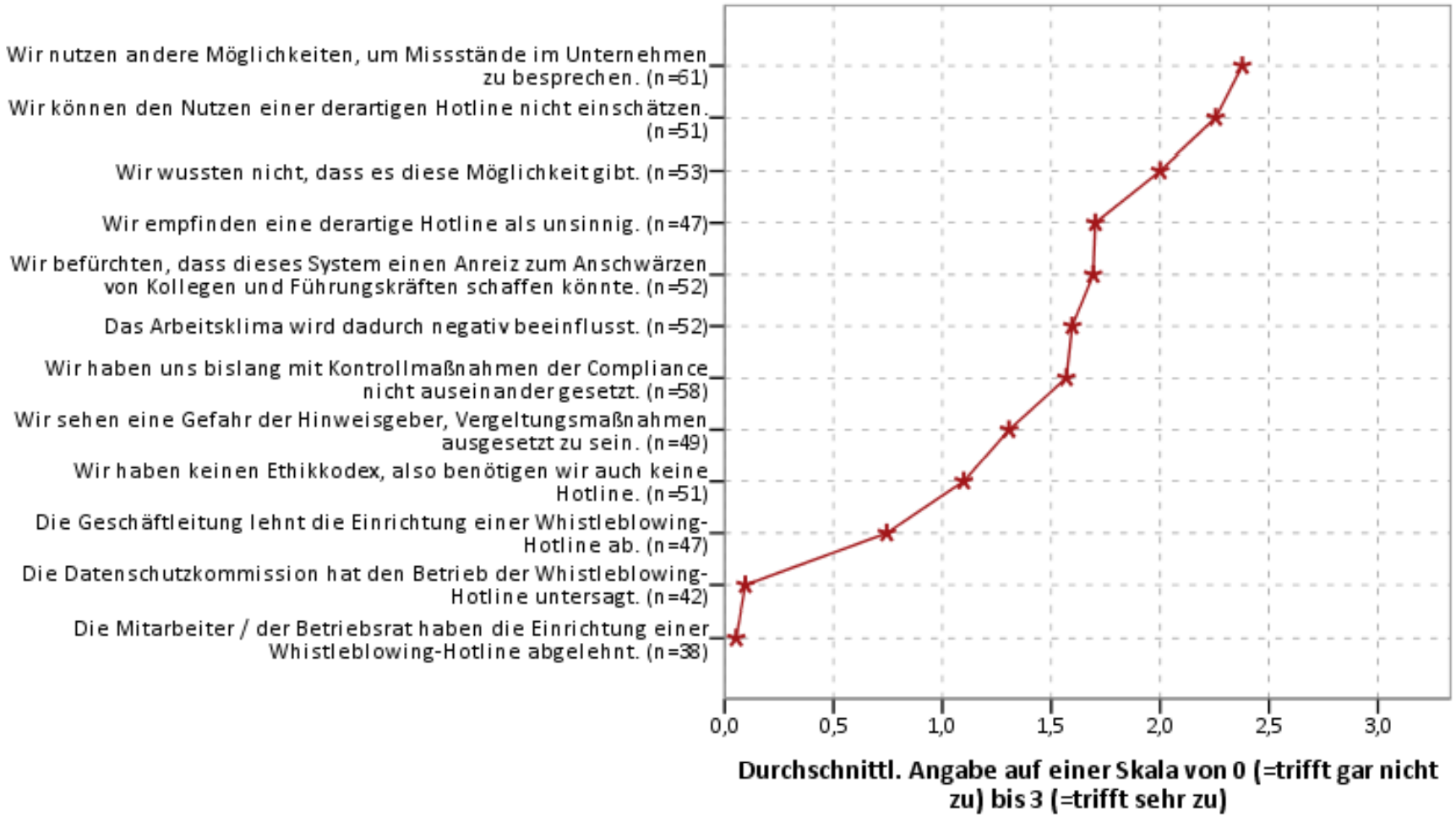


Compliance Strukturen (II)

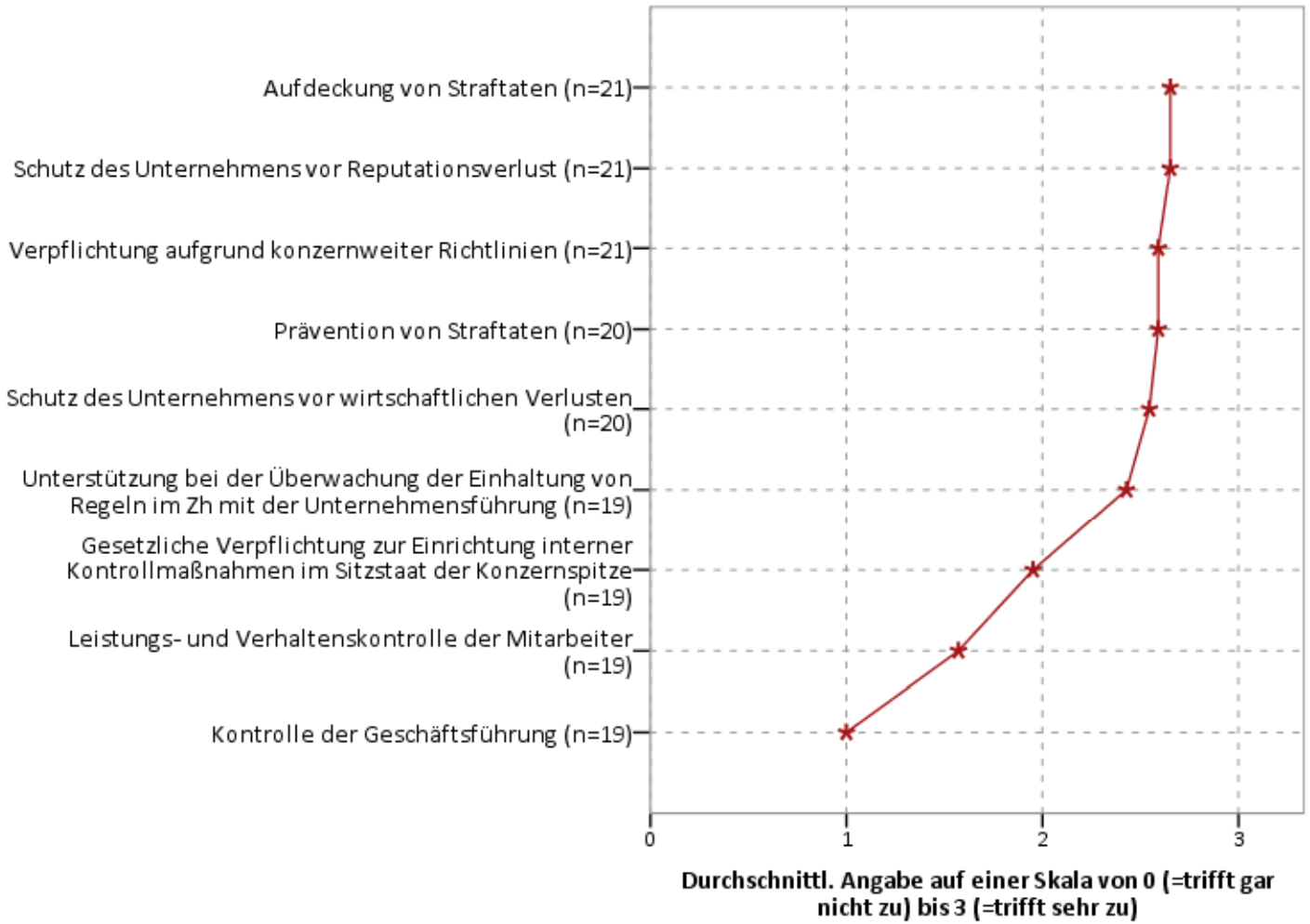
Geeignet zur Instrumentalisierung des Ethik-Kodex?



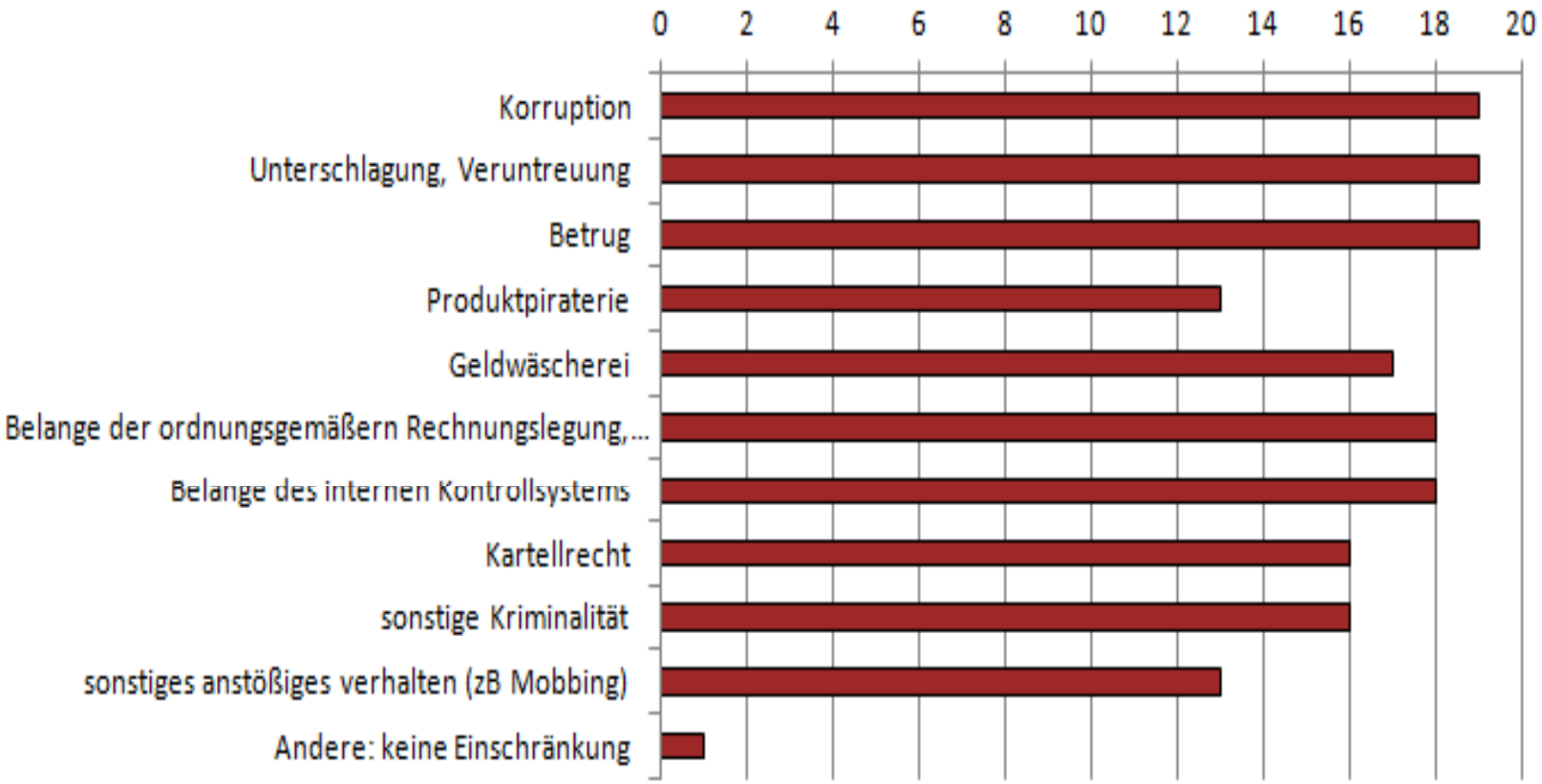
Wieso haben Sie keine Whistleblowing-Hotline?



Wieso haben Sie eine Whistleblowing-Hotline?



Wofür werden Whistleblowing-Hotlines genutzt?



Basis: Alle jene Teilnehmer, die eine Hotline implementiert haben; n=21.

Kontakt für ...

RA Dr Sonja Dürager LL.M. (IT-Law)
Donau-City-Straße 11
1220 Wien
☎ 01-260 50-125
sonja.duerager@bpv-huegel.com