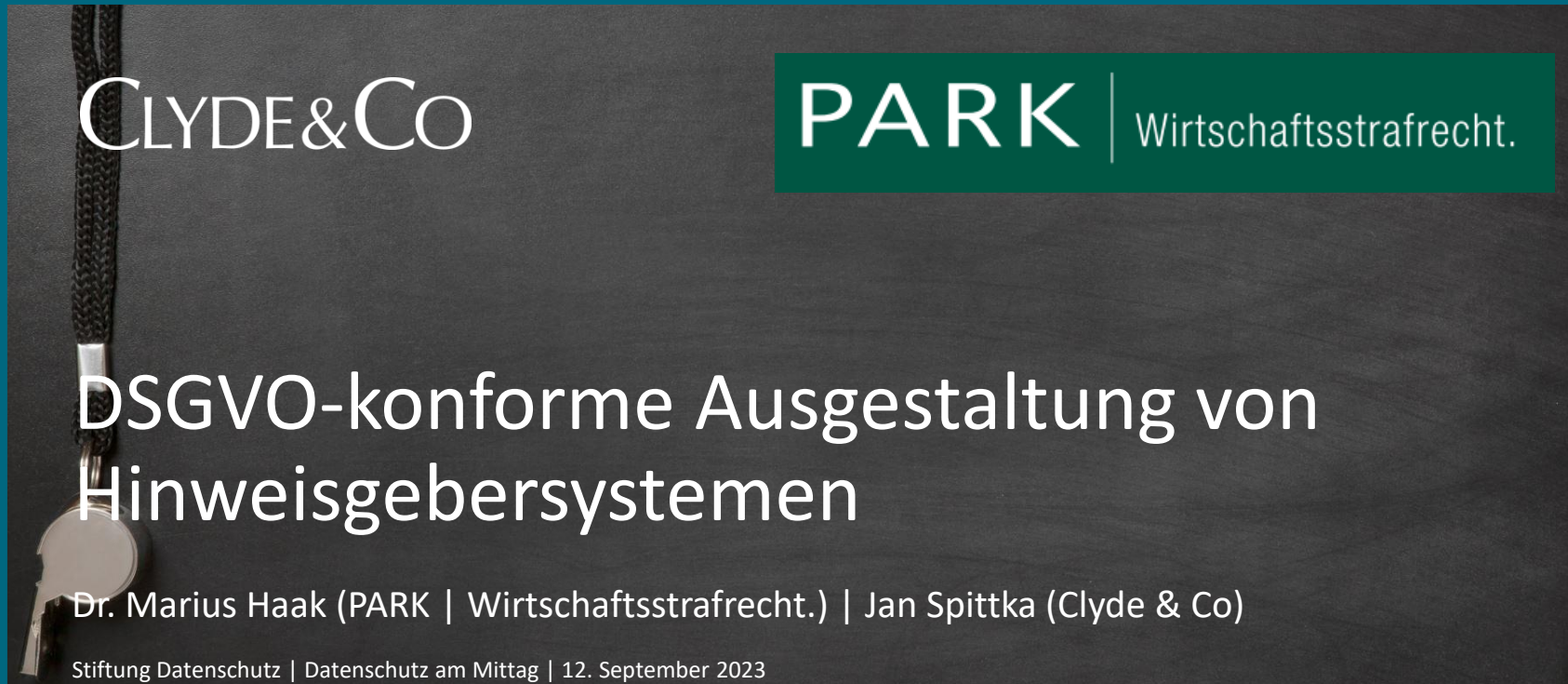


CLYDE&CO

PARK | Wirtschaftsstrafrecht.

# DSGVO-konforme Ausgestaltung von Hinweisgebersystemen

Dr. Marius Haak (PARK | Wirtschaftsstrafrecht.) | Jan Spittka (Clyde & Co)

Stiftung Datenschutz | Datenschutz am Mittag | 12. September 2023

# DSGVO-konforme Ausgestaltung von Hinweisgebersystemen

## Überblick

- Einleitung
- Einrichtung und Ausgestaltung interner Meldestellen nach dem HinSchG
- Datenschutzrechtliche Grundlagen
- Bewertung einzelner Konstellationen
- Fazit

# Einleitung

## Wenn das Hinweisgeberschutzgesetz auf die DSGVO trifft…

Bundesgesetzblatt

Teil I

2023 Ausgegeben zu Bonn am 2. Juni 2023 Nr. 140

Gesetz
für einen besseren Schutz hinweisgebender Personen
sowie zur Umsetzung der Richtlinie zum Schutz von Personen,
die Verstöße gegen das Unionsrecht melden*

Vom 31. Mai 2023

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

Artikel 1

Gesetz
für einen besseren Schutz hinweisgebender Personen
(Hinweisgeberschutzgesetz – HinSchG)

4.5.2016 DE Amtsblatt der Europäischen Union L 119/1

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

*„Bei der Verarbeitung personenbezogener Daten hat die interne Meldestelle die Vorschriften über den Datenschutz einzuhalten.“*
(BT-Drs. 20/3442, S. 79)

*„Soweit in den Erwägungsgründen der HinSch-RL von der Notwendigkeit gesprochen wird, die Ausübung bestimmter Datenschutzrechte einzuschränken, die aus der* [DSGVO] *herrühren* (…) *ist eine Regelung im HinSchG nicht veranlasst. Die für den Hinweisgeberschutz notwendigen Ausnahmetatbestände sind bereits im Bundesdatenschutzgesetz (BDSG) enthalten.“*
(BT-Drs. 20/3442, S. 36)

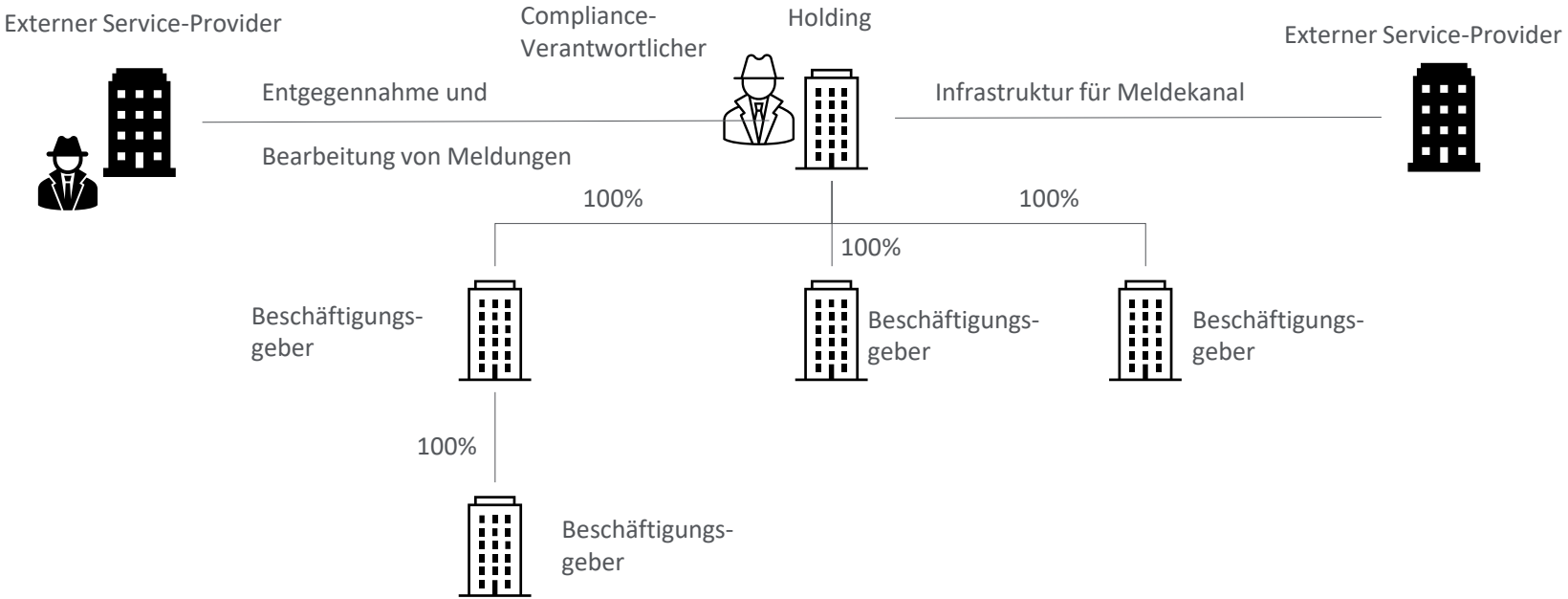
# Einrichtung und Ausgestaltung interner Meldestellen nach dem HinSchG

## Anforderungen nach HinSchG

- Pflicht besteht ab 50 Beschäftigten (§ 12 Abs. 1 HinSchG)
- Interne Meldestelle von einer bei dem Beschäftigungsgeber beschäftigten Person, einer aus mehreren beschäftigten Personen bestehenden Arbeitseinheit oder auch einem „Dritten“ betrieben werden (§ 14 Abs 1 HinSchG)
  - Wird Betrieb der internen Meldestelle an Dritten ausgelagert, verbleibt finale Verantwortlichkeit beim Beschäftigungsgeber (§ 14 Abs. 2 S. 2 HinSchG)
- Voraussetzung ist die Unabhängigkeit und Vertraulichkeit der internen Meldestelle, und auch eine personelle Kontinuität sollte vorliegen (§ 15 HinSchG).
- Aufgaben der internen Meldestelle:
  - Betreiben der Meldekanäle nach § 16 HinSchG
  - Verarbeitung und Prüfung eingehender Meldungen nach § 17 HinSchG
  - Durchführung der Folgemaßnahmen nach § 18 HinSchG

# Einrichtung und Ausgestaltung interner Meldestellen nach dem HinSchG

## Konzernkonstellationen als Herausforderung für das HinSchG



# Datenschutzrechtliche Grundlagen

## Verarbeitung personenbezogener Daten

- Mutmaßliche Täter
- Opfer und Zeugen des mutmaßlichen Verstoßes
- Hinweisgebende Person (sofern keine anonyme Meldung)
  - Keine Pflicht zur Ermöglichung anonymer Meldungen (§ 16 Abs. 1 S. 5 HinSchG)
  - Aber: Interne Meldestelle sollte auch anonym eingehende Meldungen bearbeiten (§ 16 Abs. 1 S. 4 HinSchG)
  - Anonyme Meldungen daher weiterhin möglich

> “personenbezogene Daten” [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen
>
> Art. 4 Nr. 1 DSGVO

# Datenschutzrechtliche Grundlagen

## Verteilung der datenschutzrechtlichen Verantwortlichkeit

Verhältnis zwischen Beschäftigungsgeber und interner Meldestelle?

- Auftragsverarbeitung (Art. 4 Nr. 8, 28 DSGVO)?
- Separate Verantwortlichkeit (Art. 4 Nr. 7, 1. Var. DSGVO)?
- Gemeinsam Verantwortlichkeit (Art. 4 Nr. 7, 2. Var., 26 DSGVO)?

> *„Soweit die interne Meldestelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, soll vor allem bei internen Meldestellen, die von einer Einzelperson betrieben werden, diese* ***nicht die für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften*** *sein. Soweit externe Dritte im Rahmen einer* ***Auftragsverarbeitung*** *mit der Einrichtung und dem Betreiben der internen Meldestelle beauftragt werden, sind die Vorgaben für Auftragsdatenverarbeitungen zu beachten, vergleiche Artikel 28 DSGVO.“*
>
> (BT-Drs. 20/3442, S. 79 f.)

# Datenschutzrechtliche Grundlagen

## Verteilung der datenschutzrechtlichen Verantwortlichkeit

*„Soweit die interne Meldestelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, soll vor allem bei internen Meldestellen, die von einer Einzelperson betrieben werden, diese* ***nicht die für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften*** *sein. Soweit externe Dritte im Rahmen einer* ***Auftragsverarbeitung*** *mit der Einrichtung und dem Betreiben der internen Meldestelle beauftragt werden, sind die Vorgaben für Auftragsdatenverarbeitungen zu beachten, vergleiche Artikel 28 DSGVO.“*

(BT-Drs. 20/3442, S. 79 f.)

Formulierung lautet nicht: *„Soweit externe Dritte ~~im Rahmen einer Auftragsverarbeitung~~ mit der Einrichtung und dem Betreiben der internen Meldestelle beauftragt werden, sind die Vorgaben für Auftragsdatenverarbeitungen zu beachten, vergleiche Artikel 28 DSGVO.“*

Keine Festlegung durch den Gesetzgeber, es gelten die allgemeinen Grundsätze der DSGVO

# Datenschutzrechtliche Grundlagen

## Erlaubnistatbestand

**§ 10 HinSchG**

*Verarbeitung personenbezogener Daten*

(1) Die Meldestellen sind befugt, personenbezogene Daten zu verarbeiten, soweit dies zur Erfüllung ihrer in den §§ 13 und 24 bezeichneten Aufgaben erforderlich ist. (2) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten durch eine Meldestelle zulässig, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. (3) In diesem Fall hat die Meldestelle spezifische und angemessene Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen; § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes ist entsprechend anzuwenden.

# Datenschutzrechtliche Grundlagen

## Erlaubnistatbestand

**§ 10 HinSchG**

*Verarbeitung personenbezogener Daten*

1Die Meldestellen sind befugt, personenbezogene Daten zu verarbeiten, soweit dies zur Erfüllung ihrer in den §§ 13 und 24 bezeichneten Aufgaben erforderlich ist. 2Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten durch eine Meldestelle zulässig, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. 3In diesem Fall hat die Meldestelle spezifische und angemessene Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen; § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes ist entsprechend anzuwenden.

- Bedeutung des § 10 S. 1 HinSchG ist umstritten:
    - Teilw. „*überschaubar*“ (Rüdiger/Adelberg, K&R 2023, 172, 176) oder „*deklaratorischer Natur*“ (Baade/Hößl, DStR 2023, 1265, 1267) – Lösung Art. 6 Abs. 1 lit. c DSGVO direkt i. V. M. §§ 13-24 HinSchG
    - Aber: Art. 6 Abs. 1 lit. c DSGVO kein eigenständiger Erlaubnistatbestand, Art. 6 Abs. 3 S. 1 DSGVO verlangt Rechtsgrundlage nach Unionsrecht oder dem Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt → § 10 S. 1 HinSchG ist die Schnittstelle zwischen Art. 6 Abs. 1 lit. c DSGVO und den Pflichten des HinSchG
    - Und: Ggf. Erlaubnistatbestand nach Art. 10 Abs. 1 S. 1 DSGVO erforderlich
- Daher hier vertretene Auffassung: Erlaubnistatbestand ist Art. 6 Abs. 1 lit. c DSGVO i. V. m. § 10 S. 1 HinSchG (auch für „Artikel-10-Daten“)

# Datenschutzrechtliche Grundlagen

## Erlaubnistatbestand

**§ 10 HinSchG**

*Verarbeitung personenbezogener Daten*

1Die Meldestellen sind befugt, personenbezogene Daten zu verarbeiten, soweit dies zur Erfüllung ihrer in den §§ 13 und 24 bezeichneten Aufgaben erforderlich ist. 2Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten durch eine Meldestelle zulässig, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. 3In diesem Fall hat die Meldestelle spezifische und angemessene Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen; § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes ist entsprechend anzuwenden.

- Betrieb einer internen Meldestelle erfordert oft auch die Verarbeitung besonderer Kategorien personenbezogener Daten i. S. d. Art. 9 Abs. 1 DSGVO
- Öffnungsklauseln: Art. 9 Abs. 2 lit. b DSGVO (arbeitsrechtliche Pflichten) und Art. 9 Abs. 2 lit. g DSGVO (erhebliches öffentliches Interesse)
- Maßnahme nach § 10 S. 3 HinSchG sind bei der Implementierung der internen Meldestelle zu berücksichtigen

# Datenschutzrechtliche Grundlagen

## Weitere datenschutzrechtliche Anforderungen

- **Information der betroffenen Personen (Art. 13, 14 DSGVO)**
  - Allgemeine Information und Informationen für hinweisgebende Person im Datenschutzhinweis für den jeweiligen Meldekanal
  - Information der Personen, die in der Meldung genannt werden (mutmaßliche Täter, Opfer, Zeugen)
    - Ausnahmetatbestände beachten!
      - Art. 14 Abs. 5 lit. b DSGVO: Keine Information solange Ergebnis der Untersuchung gefährdet würde
      - § 8 HinSchG beachten!
- **Auskunftsrecht (Art. 15 DSGVO)**
  - Art. 15 Abs. 4 DSGVO und § 29 Abs. 1 S. 2 BDSG bieten Möglichkeiten zum Schutz der Vertraulichkeit nach § 8 HinSchG

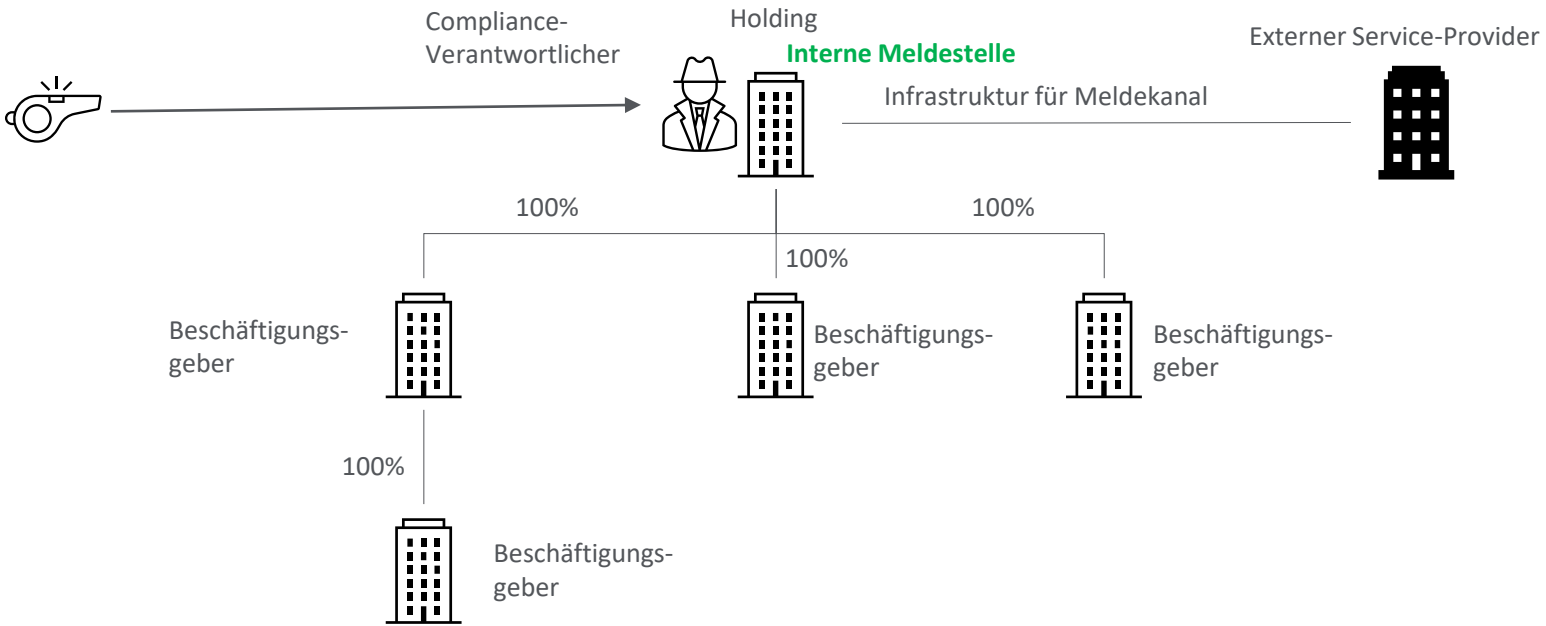
# Datenschutzrechtliche Grundlagen

## Weitere datenschutzrechtliche Anforderungen

- **Löschpflichten (Art. 17 DSGVO)**
  - Aufbewahrungspflicht des § 11 Abs. 5 HinSchG beachten!
- **Sicherheit der Verarbeitung (Art. 32 DSGVO)**
  - Rechte- und Rollenkonzept, dass Unabhängigkeit der Meldestelle (§ 15 HinSchG) sicherstellt
  - Need-to-know-Prinzip (§ 16 Abs. 2 HinSchG) muss technisch-organisatorisch abgesichert werden
  - § 10 S. 3 HinSchG beachten!
- **Datenschutz-Folgeabschätzung (Art. 35 DSGVO)**
  - Zwar (noch) keine „Blacklist-Verarbeitung“
  - Aber Potenzial für umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten
  - Verarbeitung der Meldestelle unterliegt wegen des besonders hohen Risikos für die Rechte und Freiheiten natürlicher Personen in der Regel einer DSFA.

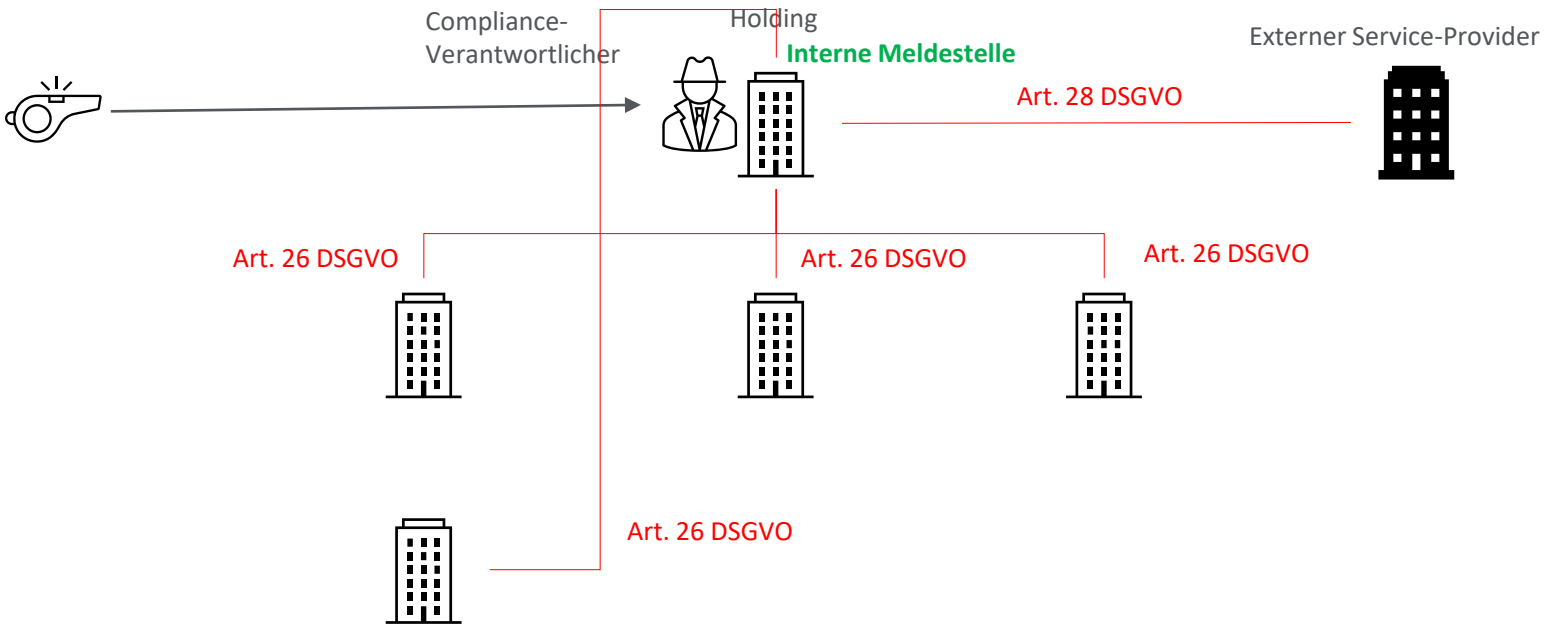
# Bewertung einzelner Konstellationen

## Fall 1: Auslagerung auf die Muttergesellschaft



# Bewertung einzelner Konstellationen

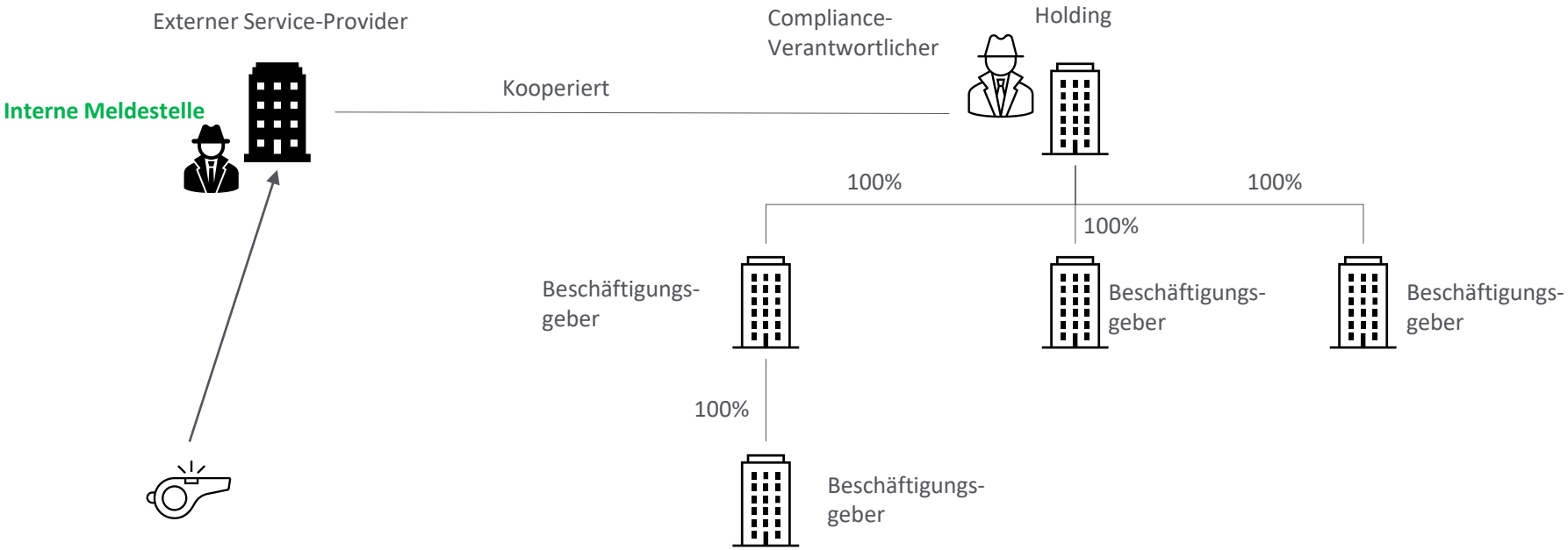
## Fall 1: Auslagerung auf die Muttergesellschaft



# Bewertung einzelner Konstellationen

## Fall 2: Vollständige Auslagerung der internen Meldestelle an externen Dritten

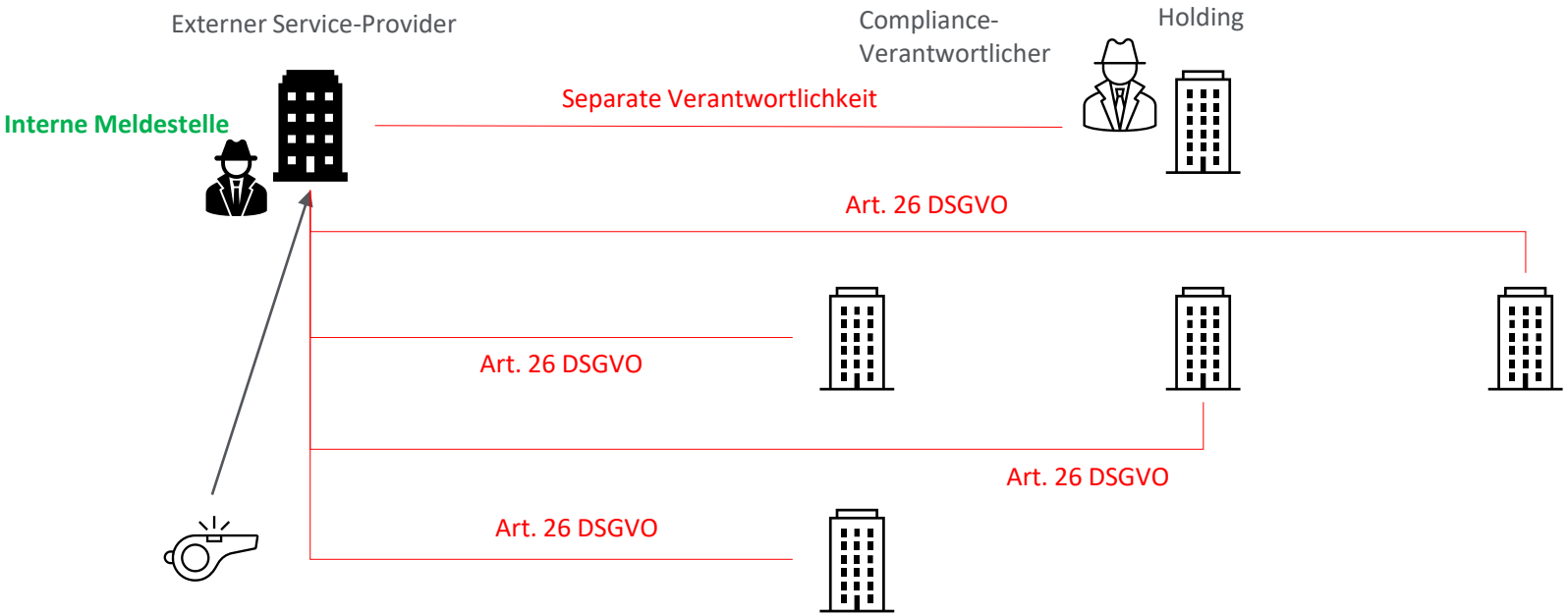
## (*Variante A – kein internes Business-Process-Outsourcing*)



# Bewertung einzelner Konstellationen

## Fall 2: Vollständige Auslagerung der internen Meldestelle an externen Dritten

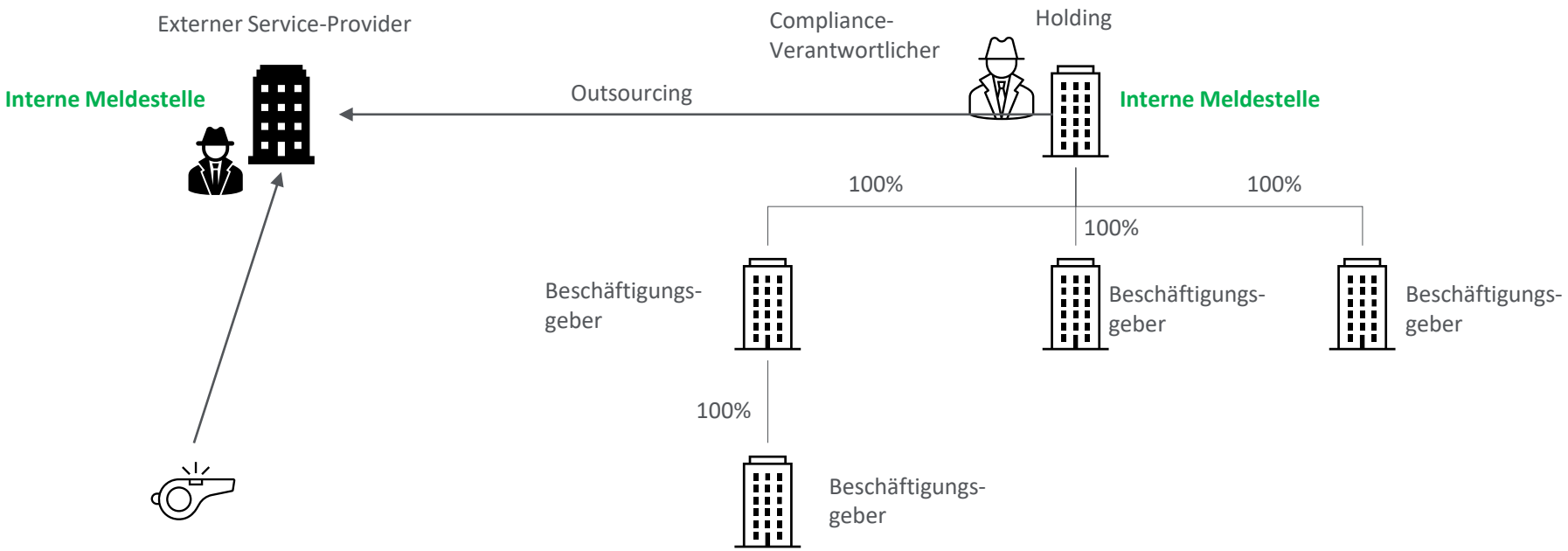
## (*Variante A – kein internes Business-Process-Outsourcing*)



# Bewertung einzelner Konstellationen

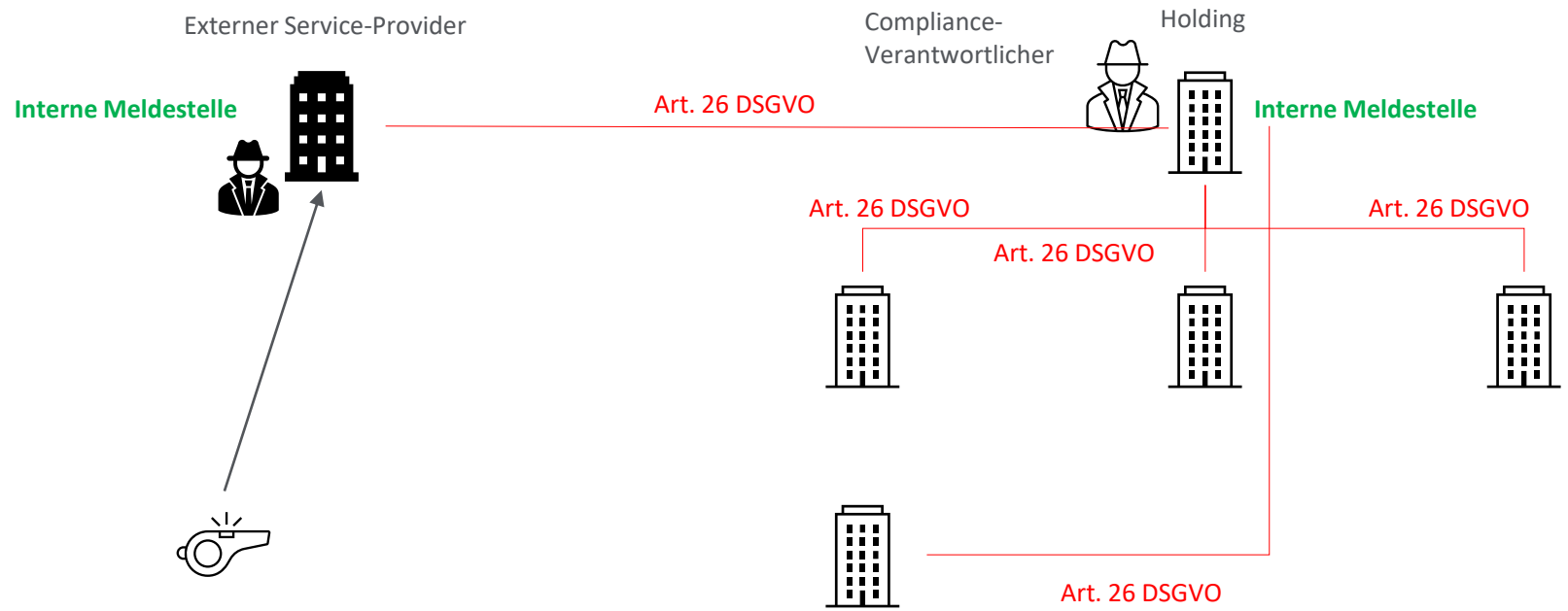
## Fall 2: Vollständige Auslagerung der internen Meldestelle an externen Dritten

## (*Variante B – internes Business-Process-Outsourcing*)



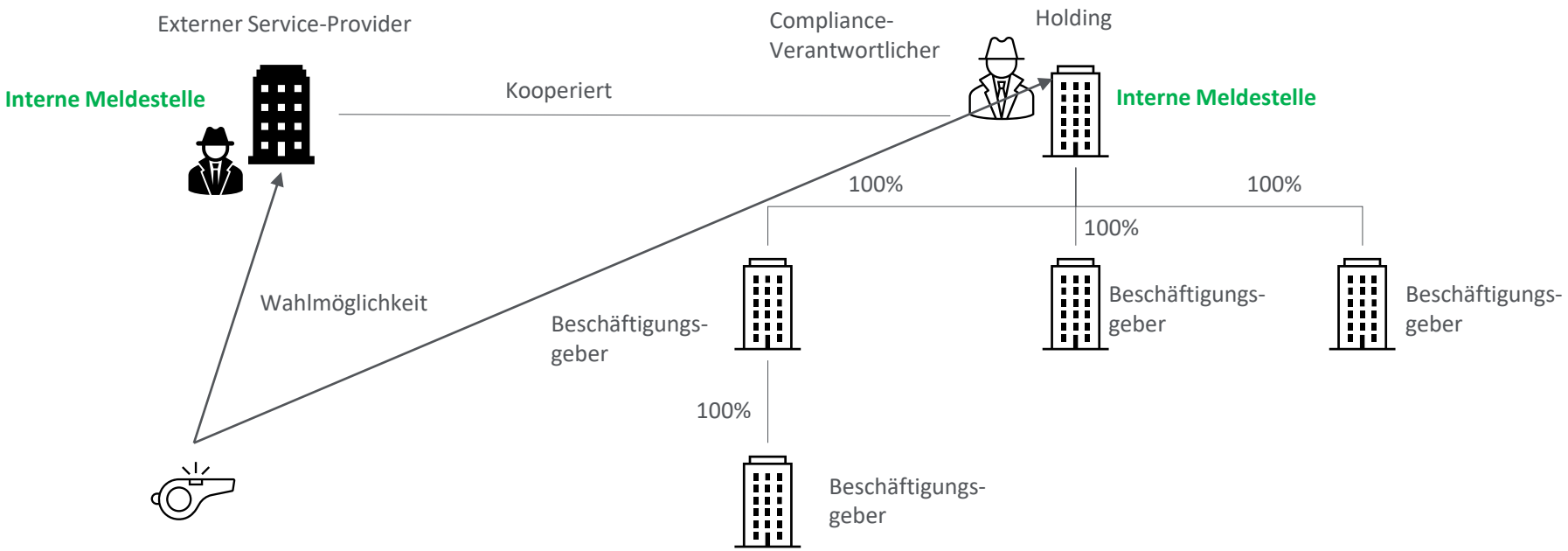
# Bewertung einzelner Konstellationen

## Fall 2: Vollständige Auslagerung der internen Meldestelle an externen Dritten (*Variante B – internes Business-Process-Outsourcing*)



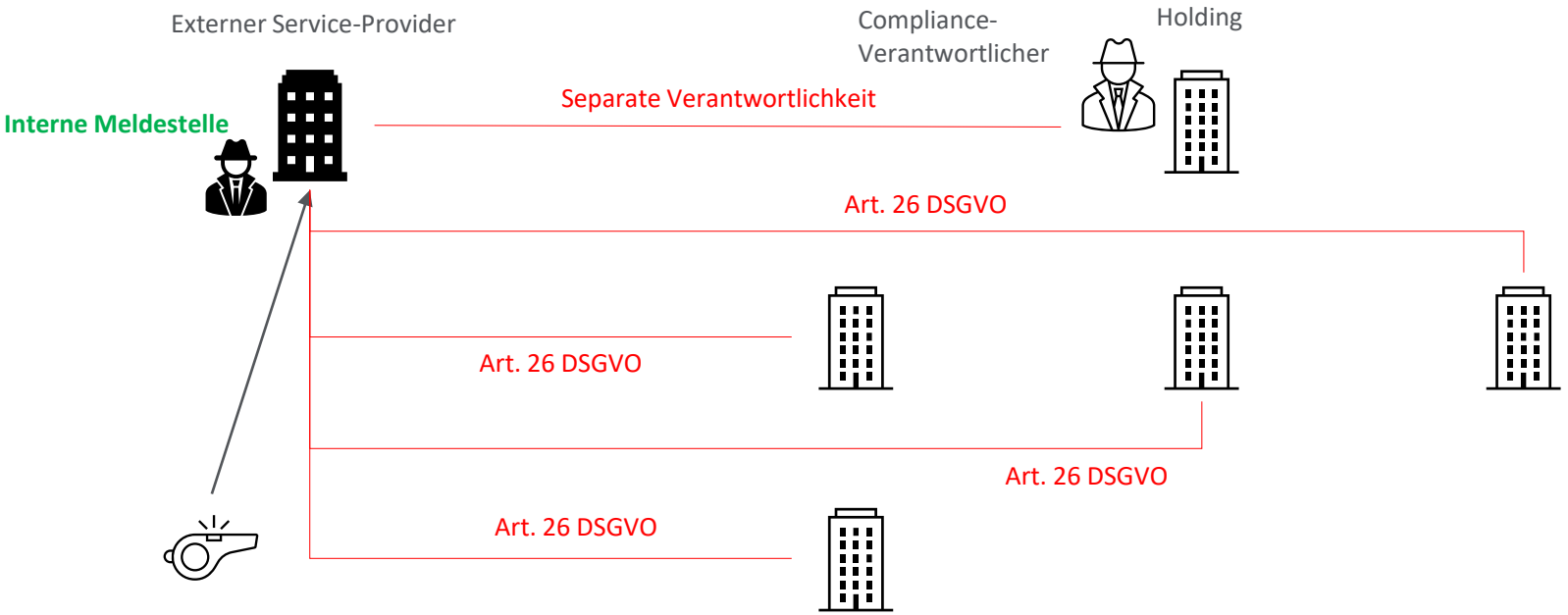
# Bewertung einzelner Konstellationen

## Fall 3: Teilweise Auslagerung der internen Meldestelle an externen Dritten



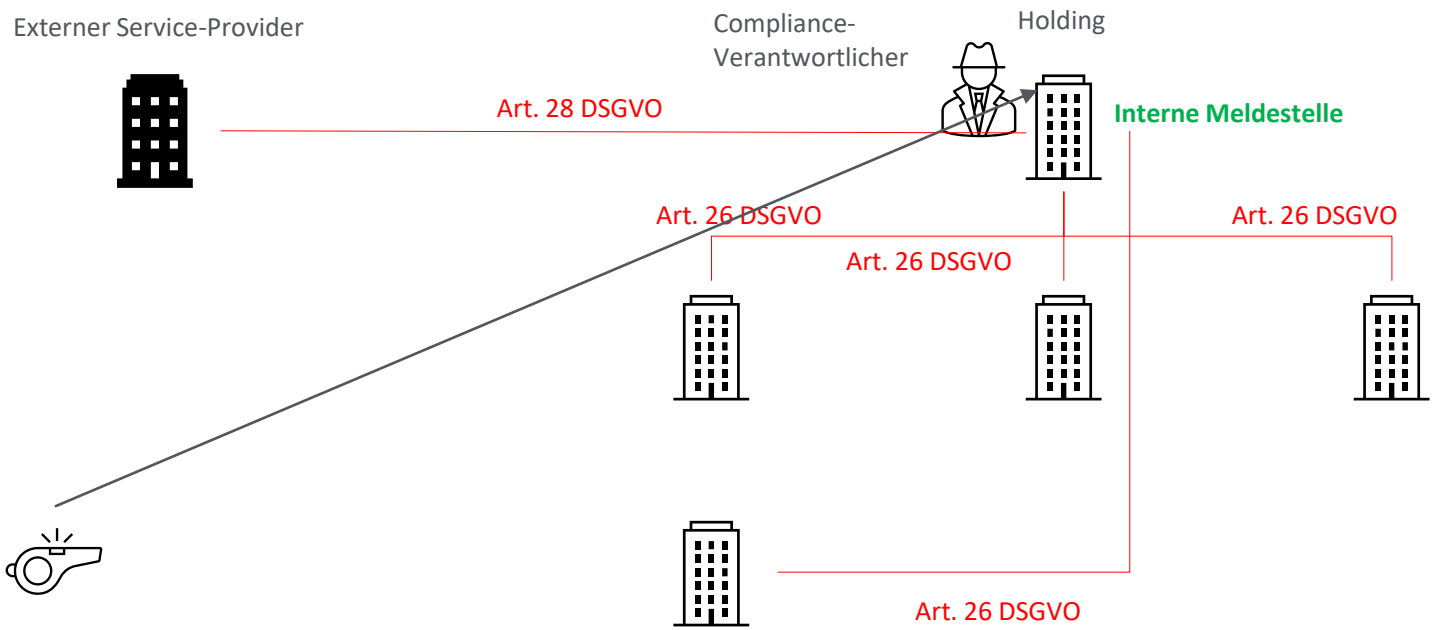
# Bewertung einzelner Konstellationen

## Fall 3: Teilweise Auslagerung der internen Meldestelle an externen Dritten



# Bewertung einzelner Konstellationen

## Fall 3: Teilweise Auslagerung der internen Meldestelle an externen Dritten



# DSGVO-konforme Ausgestaltung von Hinweisgebersystemen

## Fazit

- Einrichtung und der Betrieb einer internen Meldestelle ist für Unternehmen nicht nur hinsichtlich der Umsetzung der Anforderungen des HinSchG eine erhebliche Herausforderung.
- Datenschutz und IT-Sicherheit müssen stets mitgedacht, implementiert und dokumentiert werden.
- Wichtig ist es, die datenschutzrechtlichen Beziehungen zwischen den beteiligten Stellen im jeweiligen Einzelfall korrekt einzuordnen, da hier die entscheidende Weichenstellung zur Einhaltung der DSGVO getroffen wird.
- Angemessenes Risikomanagementsystem muss implementiert werden, das sowohl das HinSchG als auch die DSGVO berücksichtigt und alle erforderlichen Akteure einbezieht.
- Nur ein datenschutzkonformes und sicheres Hinweisgebersystemen auf Dauer von potenziellen hinweisgebenden Personen angenommen werden.

# DSGVO-konforme Ausgestaltung von Hinweisgebersystemen

## Fragen?

PARK | Wirtschaftsstrafrecht.

**DR. MARIUS HAAK**
Rechtsanwalt
Fachanwalt für Strafrecht
Certified Investigation Expert
Datenschutzbeauftragter (TÜV)

Fon +49 (231) 95 80 68 - 88
Fax +49 (231) 95 80 68 - 85
Mobil +49 (176) 609 984 65
haak@park-wirtschaftsstrafrecht.de

PARK | Wirtschaftsstrafrecht.
Rheinlanddamm 199
D - 44139 Dortmund
www.park-wirtschaftsstrafrecht.de

CLYDE&CO

**Jan Spittka**
**Rechtsanwalt | Partner**
E: jan.spittka@clydeco.com
D: +49 211 8822 8863

**Office numbers**
T: +49 211 8822 8800
F: +49 211 8822 8898

Clyde & Co
Dreischeibenhaus 1
40211 Düsseldorf
Germany