RIMÔN
FALKENFORT

„Whistleblowing Systems“

September 2021

WORUM GEHT ES?

WORUM GEHT ES?

RIMÔN FALKENFORT

Während in der UK (seit 2016 FCA Rules) und in Frankreich (seit 2018 Sapin II) seit Jahren Antikorruptions-Gesetze samt Whistleblowing Protection existieren, besteht in Deutschland bis heute kein ausdrücklicher gesetzlicher Schutz von Hinweisgebern.

Das Thema ist seit Jahren immer wieder gut für Schlagzeilen quer durch die gesamte Presselandschaft. Von den zunehmend lauter werden Kritikern wurde dabei allerdings gerne übersehen, dass in Deutschland sehr wohl Schutzrechte bestehen. Angefangen von strikten Kündigungsschutzgesetzen, Beschwerderechten und Verschwiegenheitsverpflichtungen:

- den in der EU unbestritten strengsten Kündigungsschutz von ArbeitnehmerInnen gemäß **KSchG**,
- strenge Anforderung an Arbeitsschutz gemäß **ArbSchG**,
- und Gleichbehandlungsgrundsätze gemäß **AGG**, sowie
- zumindest einzelne Verschwiegenheitsverpflichtungen nach **AktG** und **UWG**.

SCHON BESTEHENDE REGELUNGEN?

RIMÔN FALKENFORT

Darüber hinaus bestehen in Deutschland im Finanzdienstleistungsbereich sehr wohl auch auf Hinweisgeber zielende Regelungen zum Geschäftsgeheimnis gemäß **GeschGehG** und **FinDAG**. § 4d FinDAG sieht bereits aktuell die Einrichtung von Meldesystemen und den Schutz von Hinweisgebern vor.

Aber dennoch, richtig ist, dass bis heute in Deutschland kein einheitlicher Schutz von Hinweisgebern gesetzlich verankert ist; insbesondere besteht aktuell in Deutschland kein besonderer Kündigungsschutz für Whistleblower.

Angesichts der bevorstehenden Bundestagswahl verbleibt wenig Zeit, die EU-Whistleblower-Richtlinie fristgerecht in deutsches Recht umzusetzen.

Für Unternehmen besteht Handlungsbedarf!

WAS MACHT BERLIN?

RIMÔN FALKENFORT

Der Termin steht schon seit langem fest: Spätestens am **17. Dezember 2021** muss die EU-Whistleblower-Richtlinie ((EU) 2019/1937), die am 16. Dezember 2019 in Kraft getreten ist, von den EU-Mitgliedstaaten in nationales Recht umgesetzt sein.

Der Entwurf des Hinweisgeberschutzgesetzes (**HinSchG**) wurde Ende April 2021 von der Regierung zurückgewiesen. Das Thema hängt im Gesetzgebungsverfahren fest – was nicht verwundert, sah der Referentenentwurf doch Regelungen vor, die weit über die EU-Vorgaben hinausgingen.

WAS PASSIERT WENN NICHT?

RIMÔN FALKENFORT

Es ist mehr als fraglich, ob angesichts der Bundestagswahl und vordringlicherer Themen in Berlin noch Zeit bleibt, in Deutschland ein Gesetz auf den Weg zu bringen.

Bei Verstreichen der Frist droht aus Brüssel ein Vertragsverletzungsverfahren und uU für Unternehmen ohne Hinweisgebersysteme Sanktionen und Haftungsrisiken.

Unternehmen sind daher gut beraten, sich rechtzeitig mit dem Thema HinSchG auseinander zu setzen, insbesondere wenn sie noch kein internes Hinweisgebersystem eingerichtet haben.

WER SOLLTE HANDELN?

RIMÔN FALKENFORT

Erfahrungen bei der Umsetzung der Datenschutz-Grundverordnung (**DSGVO**) haben gezeigt, dass eine rechtzeitige Vorbereitung von betrieblichen Compliance Maßnahmen dringend angezeigt ist; ansonsten drohen Haftungsrisiken und Bußgelder.

Handlungsbedarf besteht für

- alle Finanzdienstleister unabhängig von ihrer Mitarbeitergröße,
- Unternehmen ab 50 Arbeitnehmern, einschließlich freier Mitarbeiter, sowie
- Unternehmen mit einem Umsatz ab € 10 Mio. p.a.;

- für Unternehmen mit 50 aber weniger als 250 Mitarbeitern gilt eine um zwei Jahre verlängerte Frist zur Umsetzung bis zum **17. Dezember 2023**.

Es gibt nicht wenige Stimmen, die im Fall eines Verstreichens der Frist von einer unmittelbaren Anwendbarkeit der EU- Richtlinie ausgehen…

WAS SIEHT DIE EU RICHTLINIE VOR?

RIMÔN FALKENFORT

Eine unmittelbare Anwendbarkeit der EU- Richtlinie würde bedeuten:

- it applies to workers, self-employed individuals, shareholders, contractors and subcontractors,
- former employees and workers, as well as job applicants;

- employers with 50 or more employees must establish internal channels and procedures for whistleblowers
- to make a report and for the employer to follow up;

- reporting channels must be secure and
- ensure the whistleblower's identity is kept confidential;

- whistleblowers must be given feedback by the employer within three months;

- their identity cannot be disclosed without their explicit consent;
- whistleblowers will be protected against retaliation and will be immune from civil liability relating to their use of information (e.g. confidentiality claims).

WAS SIND DIE ZIELE DES *HinSchG*?

ZIELE DES HINSCHG?

RIMÔN FALKENFORT

Nach dem (verworfenen) Referentenentwurf des BMJV sollen Arbeitgeber:

- Meldesysteme aus internen und externen Meldekanälen schaffen, damit
- Hinweisgeber Verstöße gegen
    - EU-Recht,
    - OWiG oder
    - Straf-Recht melden können;
- mit dem Zweck einer besseren Aufdeckung und Unterbindung von rechtswidrigen Handlungen;
- zum besseren Schutz von Hinweisgebern gegen Repressalien, sowie
- ebenfalls zum Schutz der Unternehmen vor falschen Hinweisen.

.

INHALTE DES HINSCHG?

RIMÔN FALKENFORT

Wesentliche Inhalte umfassen:

- Zugänglichkeit von Meldestellen für alle MitarbeiterInnen,
- Besetzen der Meldestellen mit geschultem Personal;

- unabhängige Entscheidungsfindungen der Meldestellen, bei Schutz der Vertraulichkeit sowohl der Hinweisgeber als auch der durch die Meldung Betroffenen;

- Einrichtung von Fristabläufen,
- Dokumentationsverpflichtungen sowie
- Einleiten von Folgemaßnahmen.

.

WAS IST ZU TUN?

WAS IST ZU TUN?

RIMÔN FALKENFORT

Unternehmen, die bisher

- weder eine „Hotline“ für Whistleblower,
- noch andere interne Hinweisgebersysteme eingerichtet haben,

sollten sich mit folgenden Themen beschäftigen:

- Einrichtung interner Meldekanäle,
- Zugänglichkeit für alle Mitarbeiter;

Unabhängigkeit von Meldestellen mit geschultem Personal, unternehmensintern oder extern durch Dritte, z.B. durch RAe oder andere Ombudspersonen.

WAS IST ZU BEACHTEN?

RIMÔN FALKENFORT

Einrichtung von Meldesysteme unter

- Wahrung der Vertraulichkeit der Hinweisgeber, sowie
- der Verpflichtung, auch anonymen Hinweisen nachzugehen, bei

- gleichzeitigem Schutz der Mitarbeiter vor Repressalien und
- Schutz der Arbeitgeber vor falschen Hinweisen.

Eine Überprüfung - und ggf. Änderung - bereits bestehender Hinweisgebersysteme ist mehr als ratsam, unter – gegebenenfalls –notwendiger Wahrung bestehender Mitbestimmungsrechte der Betriebsräte nach **§ 87 I Nr. 1 und 6 BetrVG**.

WORAN SOLLTE MAN DENKEN?

RIMÔN FALKENFORT

Wie bei allen Compliance Themen gilt:

Eine erfolgreiche Einführung von Meldesystemen ist auch (und gerade) eine Frage der Unternehmenskultur.

Ein klares Kommittent aus der Vorstandsetage hilft bei der Umsetzung im Unternehmen. Letztendlich wird nur eine ausreichend breite Akzeptanz in der Belegschaft zum Erfolg von Hinweisgebersystemen führen.

Gerade in Deutschland bestehen immer noch Bedenken der Belegschaft. Whistleblower werden immer noch oft mit Denunzianten gleichgesetzt. Es empfiehlt sich daher, Fragen der Mitarbeiter ernst zu nehmen nach:

- Sicherung der Vertraulichkeit und Anonymität,
- Vorbehalten gegen umfängliche Aufklärungen und echte Investigationen
- sowie Ängsten gegen Repressalien **(„verliere ich meinen Job …“)**.

.

WER IST EINZUBINDEN?

RIMÔN FALKENFORT

Von Anfang an sind unternehmensintern folgende Abteilungen einzubinden:

- HR und Compliance Abteilungen,
- IT Abteilungen und (sofern im Haus)
- der Datenschutzbeauftragte.

Vor allem gilt es, bestehende Investigations-Prozesse zu überprüfen. Fragen werden zu beantworten sein wie:

- Sollen Hinweise zentral erfasst oder
- direkt zur „betroffenen“ Stelle geleitet werden?

- Bestehen storage and delete Prozesse für erhobene und gespeicherte Daten?
- Wie transparent wird mit dem Hinweisgeber nach Einleiten des Reports umgegangen?

DIGITALE HINWEISGEBERSYSTEME?

PRO UND CONS

RIMÔN FALKENFORT

Unternehmen nutzen in aller Regel folgende Wege, die sich vom einfachen „Kummer-Briefkasten“ bis zur online Plattform unterscheiden:

- Briefkasten vor Ort im Betrieb: Hinweise erfolgen in Papierform,
- zentraler Email Account: hierher werden Hinweise gemailt,
- lokale Telefonhotlines mit Voicemail/ Recording Devices,
- ob intern oder über externe Call-center;

- Anlaufstelle über einen externen, unabhängigen Ombudsmann, oder
- Einrichten einer digitalen online Plattform, die vertraulich und anonym genutzt werden kann (die **PUMA** „SpeakUP“ Plattform erlangte eine gewisse Bekanntheit in der Öffentlichkeit).

Letzteres wird in vielen Fällen Vorteile mit sich bringen, wird aber uU in klassischen Produktionsbetrieben Anwendungsbarrieren schaffen.

ZEITINTENSIV UND KOSTSPIELIG?

RIMÔN FALKENFORT

Unternehmen sollten nicht den Aufwand und insbesondere den erforderlichen Zeitumfang unterschätzen:

- von der Definition der Reporting Kategorien,
- der Eskalation Prozesse,
- über das Testen, den „dry-run“ bis
- zum eigentlichen „Launch“ des Meldesystems.

Die interne Kommunikation und das erfolgreiche „Verkaufen“ eines Meldesystems erfordert in aller Regel externen Sachverstand und viel Erfahrung. Die Einrichtung von Telefonhotlines sowie die Einrichtung digitaler Hinweisgebersysteme für die schriftliche Abgabe von Hinweisen werden in der Praxis meist kombiniert.

Meldesysteme werden in der Zukunft wichtiger Bestandteil von Compliance Prozessen sein.

.

WOMIT IST IN ZUKUNFT ZU RECHNEN?

BEISPIELE AUS DEN USA?

RIMÔN FALKENFORT

Werden wir in Deutschland mit finanziellen Anreizen für Hinweisgeber rechnen müssen?

"200 Millionen Dollar für Deutsche-Bank-Whistleblower – Amerikanische Behörde zahlt Rekordsumme"
Nach dem Bericht der FAZ (FAZ vom 23. Oktober 2021) zahlte allein die Deutsche Bank im Zuge der Aufklärung in den USA Strafen und Bußgelder iHv 2,5 Milliarden Dollar (USB 1,2 Milliarden EUR und britische Banken dreistellige Millionenbeträge. Die EU- Kommission verhängte zusätzlich Rekordstrafen gegen die beteiligten Banken iHv 1,7 Milliarden EUR.

Die ***Commodity Futures Trading Commision/ CFTC*** zahlt seit dem Jahr 2010 Belohnungen an Whistleblower bei der Aufklärung von krummen Finanzgeschäften, ebenso wie die ***SEC*** (dort betrug die bisher höchste Belohnung 130 Millionen EUR.

Weder die EU-Richtlinie noch das **HinSchG** sehen das vor.

Aber angesichts des vorgesehenen Wahlrechts für Hinweisgeber, interne oder externe Meldesystem zu nutzen, werden sich Unternehmen gut überlegen, wie sie ihre Belegschaft dazu bringen, vorrangig interne Kanäle zu nutzen.

Man kann hier u.a. an ein Ausloben von Prämienzahlungen denken.

ABGRENZUNGEN?

RIMÔN FALKENFORT

Mit welchen Abgrenzungen des HinSchG zu GeschGehG und VerSanG ist zu rechnen?

Nach dem letzten Stand des HinSchG eröffnet nur ein rechtswidriges Fehlverhalten in Form von Handlungen und/oder Unterlassungen den sachlichen Anwendungsbereich des HinSchG.

Ein lediglich „unethisches“ Verhalten genügt nicht.

Eine Offenlegung und Weiterleitung von Geschäftsgeheimnissen soll nach dem HinSchG nur dann erlaubt sein, wenn der Whistleblower hinreichenden Grund zu der Annahme hatte, dass die Weitergabe oder Offenlegung notwendig ist, um einen Verstoß aufzudecken.

Es bliebe folglich beim Ausnahmetatbestand des § 5 Nr. 2 GeschGehG – auch im Rahmen des **HinSchG**.

COMPLIANCE ANFORDERUNGEN?

RIMÔN FALKENFORT

Müssen wir im Zeitalter des „*digital workplace*“ mit steigenden Compliance Anforderungen rechnen?

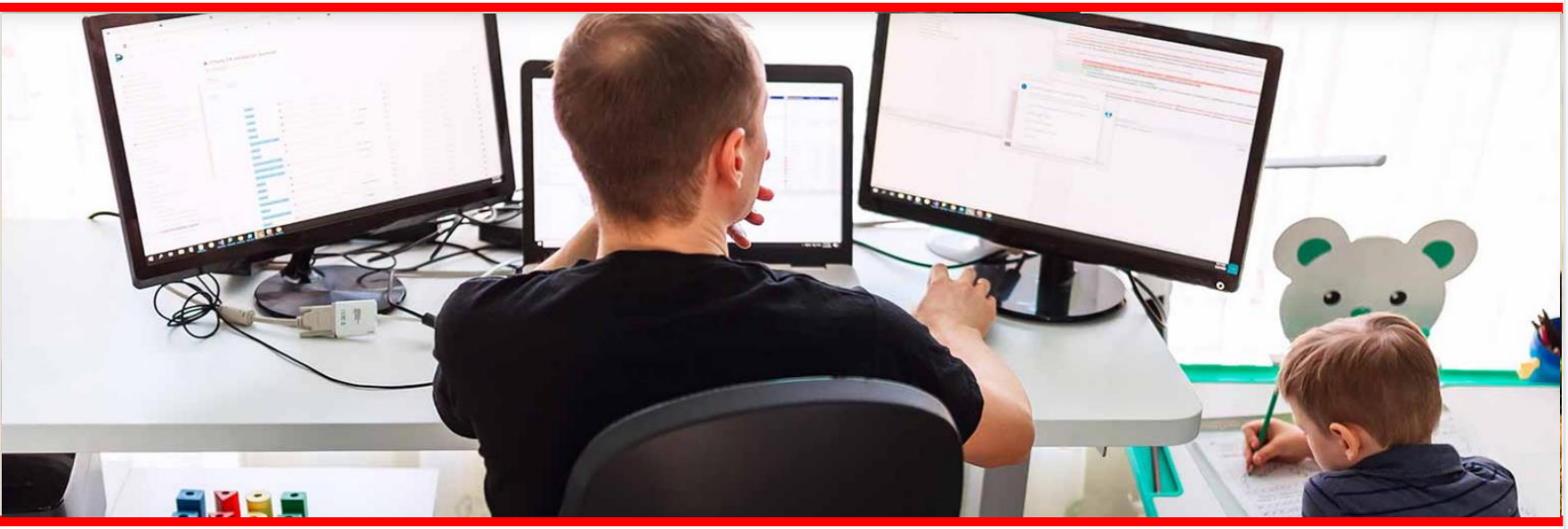
Ganz allgemein wird man nicht darum herum kommen, Meldesysteme in bereits bestehende Compliance Abläufe eng einzubinden.

Dass diese sich laufend – und in immer kürzer werdenden Zeiträumen – an den sich rasant entwickelnden Anforderungen der digitalen Wirklichkeit anpassen müssen, scheint unbestritten.

.

LABOR & EMPLOYMENT

LABOR & EMPOYMENT



SELECTED EXPERIENCE

- Viskase Companies Inc. On complex restructuring measures, including mass dismissals and collective bargaining matters
- EIT Health e.V. on setting up new management structures; C-level coaching
- GfK SE on D&O matters, C-level coaching
- MAS Malaysian Airlines on its complete shutdown of all its German hubs
- HB Fuller in relation with their acquisition of Swiss Forbo plants in Germany

* Includes work for other law firms

- ✓ Future of Labor Law
- ✓ Regulatory Changes
- ✓ Mindfulness at the Workplace
- ✓ Communicating in times of Crisis
- ✓ Works Council Issues
- ✓ Union matters
- ✓ Labor Compliance
- ✓ Diversity Issues
- ✓ Risk Management
- ✓ Whistleblowing Systems
- ✓ Remuneration Structures
- ✓ Data Protection

TEAM

RIMÔN FALKENFORT

Michael Magotsch, LL.M. (Georgetown)

Partner

Rechtsanwalt

Frankfurt am Main

Germany

Michael Magotsch has over 30 years of experience in advising global companies in all aspects of German labor and employment law. His practice focuses on national and cross-border restructurings, acquisitions, redundancies and outsourcing measures.

He also advises C-level executives in transition or exit scenarios as well as supervisory boards in sensitive disputes with C-level executives.

Michael held various management positions for other law firms.

He was Coudert Brothers` Head of the EU Employment Practice as well as Country Managing Partner for Germany until 2005. He started DLA Piper`s Frankfurt office and was Office Managing Partner until 2009.

Michael Magotsch
Partner

+49 69-589962-413

michael.magotsch@rimonlaw.de

Save contact

- Labor & Employment
- Compliance
- M&A/Corporate
- Restructuring

ABOUT US

RIMÔN FALKENFORT

★ Current Rimon offices

☆ Casablanca, Dubai, Hong Kong offices Coming soon!

● Rimon Global Alliance, our network of trusted lawyers and law firms throughout the world

RIMÔN
FALKENFORT

www.rimonlaw.de