



## WHISTLEBLOWER-RICHTLINIE – HANDLUNGSBEDARF FÜR UNTERNEHMEN

In der Vergangenheit hielt die Europäische Kommission bereits mehrfach fest, dass der Schutz von Hinweisgebern von zentraler Bedeutung für die Verhütung von Fehlverhalten von Unternehmen und zur Wahrung der öffentlichen Interessen ist. Die Europäische Kommission erklärte, dass der wichtigste Grund, weshalb Arbeitnehmer festgestellte Fehlverhalten nicht melden und somit Schäden nicht verhindert werden, Angst vor rechtlichen und finanziellen Konsequenzen sei. Der Schutz von Hinweisgebern wurde somit seitens der Europäischen Union als essentiell erkannt.

Am 16.12.2019 trat die sogenannte „Whistleblower-Richtlinie“ (RL (EU) 2019/1937) in Kraft, welche binnen 2 Jahren in nationales Recht umzusetzen ist.

Die Richtlinie soll einheitliche Mindeststandards zum Schutz von Hinweisgebern festlegen, um Fehlverhalten zu verhindern und die öffentlichen Interessen zu schützen. Dadurch soll es zu einer Stärkung des Investitionsklimas und des Glaubens in öffentliche Institutionen kommen.

Die Umsetzung der Anforderungen dieser Richtlinie und des darauf beruhenden nationalen Rechts, wird viele Unternehmen, Behörden und deren Compliance Organisationen vor neue Herausforderungen stellen. In weiterer Folge stellen wir kurz dar, was auf Unternehmen und deren Compliance Organisationen zukommt.

### I. SCHUTZBEREICH

Die Richtlinie schützt jene Hinweisgeber (Whistleblower), die im privaten oder öffentlichen Sektor tätig sind und im beruflichen Kontext Informationen über Verstöße gegen EU-Recht erlangen.

Der Begriff des Hinweisgebers ist sehr weit gefasst. Er umfasst Arbeitnehmer, Beamte, Selbstständige, Gesellschafter sowie Personen, die einem Verwaltungs-, Leitungs- oder Aufsichtsorgan eines Unternehmens angehören, aber auch Praktikanten. Umfasst sind ebenfalls Dienstleister und Lieferanten. Für den Begriff des Hinweisgebers ist es unerheblich, ob ein zukünftiges, gegenwärtiges oder vergangenes Vertragsverhältnis mit dem Unternehmen vorliegt.

Eine wesentliche Voraussetzung für den Schutz des Hinweisgebers ist, dass er – bei seiner Meldung – hinreichenden Grund zur Annahme hatte, dass die gemeldete Information über Verstöße zum Zeitpunkt der Meldung der Wahrheit entsprechen und Rechtsgebiete betreffen, welche von der Richtlinie geschützt werden.

Der Hinweisgeber muss also gutgläubig sein, um in den Genuss des Schutzes der Richtlinie zu kommen. Die Richtlinie sieht vor, dass nur Meldungen von Verstößen gegen EU-Recht geschützt werden.

Diese Beurteilung wird für einen Hinweisgeber nicht leicht sein und so ist abzuwarten, ob der



ationale Gesetzgeber nicht auch Verstöße gegen nationales Recht in den Schutzbereich aufnimmt, um so das Risiko einer Falsch-Beurteilung durch potentielle Hinweisgeber zu verringern.

## II. SCHUTZ VOR REPRESSALIEN

Die Richtlinie will sicherstellen, dass potentielle Hinweisgeber vor jeglichen Repressalien geschützt werden. Solche Repressalien umfassen zum Beispiel Entlassungen, Suspendierungen, Diskriminierungen, Gehaltsminderungen, Drohungen und/oder die Aufnahme auf „schwarze Listen“ für Lieferanten.

Der Schutz vor Repressalien soll unter anderem dadurch sichergestellt werden, dass Mitgliedstaaten durch deren Behörden über den Schutz von Hinweisgebern ausreichend zu informieren haben und für Opfer von Repressalien Beratungen sicherstellen. Weiters ist in Gerichtsverfahren eine Beweislastumkehr vorzusehen. Der Arbeitgeber bzw. der Auftraggeber muss beweisen, dass eine Benachteiligung des Hinweisgebers nicht aufgrund einer Meldung des Hinweisgebers erfolgte. Weiters sind Hinweisgeber, die gegen vertragliche oder gesetzliche Informationsbeschränkungen verstoßen, von der Haftung auszunehmen.

## III. VERPFLICHTENDE MELDEKANÄLE FÜR UNTERNEHMEN

Herzstück der Richtlinie ist die Verpflichtung für Unternehmen des privaten und öffentlichen Sektors, sowie für Behörden zuverlässig funktionierende interne Meldekanäle einzurichten, damit Hinweisgeber Verstöße unter Geheimhaltung ihrer Identität melden können.

Zur Einrichtung eines internen Meldesystems sind all jene Unternehmen verpflichtet,

- die mehr als 50 Mitarbeiter beschäftigen oder
- deren Jahresumsatz EUR 10 Millionen übersteigt.

Weiters sind Gemeinden ab 10.000 Einwohnern zur Einrichtung eines internen Meldesystems verpflichtet.

Juristische Personen des öffentlichen Sektors, einschließlich Stellen, die im Eigentum oder der Kontrolle einer solchen juristischen Person stehen, haben jedenfalls ein internes Meldesystem einzurichten.

Unternehmen mit mehr als 250 Mitarbeitern haben diese internen Meldekanäle bis spätestens 17. Dezember 2021 umzusetzen. Unternehmen mit einer Mitarbeiterzahl zwischen 50 und 250 haben hierzu bis zum 17. Dezember 2023 Zeit.

Hinweisgeber sollen in solch einem internen Meldekanal der Unternehmen die Möglichkeit erhalten Meldungen entweder schriftlich über ein Online-System, einen Briefkasten oder per Postweg abzugeben und/oder mündlich per Telefon-Hotline oder Anrufbeantwortersystem.

Unabhängig von der Art des Meldesystems, muss das Unternehmen sicherstellen, dass die Identität des Hinweisgebers und von in der Meldung genannten Personen immer geschützt werden.

Innerhalb eines Unternehmens ist die am besten geeignete Person zum Erhalt und zur Nachverfolgung der Meldungen zu bestimmen (z.B. Compliance, Rechtsabteilung etc.). Prinzipiell kann auch ein externer Dienstleister Empfänger und Bearbeiter der Meldungen sein. Unbefugten Mitarbeitern ist der Zugriff auf das Meldesystem jedenfalls zu verwehren. Alle personenbezogenen Daten müssen von Unternehmen DSGVO-konform verarbeitet werden.

Nach Erhalt einer Meldung muss dem Hinweisgeber vom Unternehmen bzw. der dazu bestimmten Person binnen 7 Tagen eine Erhaltbestätigung zugestellt werden und binnen einer weiteren Frist von 3 Monaten ist der Hinweisgeber zu informieren, welche Folgemaßnahmen auf Grundlage seiner Meldung getroffen



wurden. Dies erfordert im Unternehmen eine strenge Fristenverwaltung.

Unternehmen sind weiters verpflichtet, ihren Mitarbeitern Informationen über den unternehmensinternen Meldeprozess und über den alternativ möglichen Meldeprozess an die zuständige Behörde zur Verfügung zu stellen. Diese Informationen müssen leicht zugänglich und leicht verständlich sein. Alle Vorgänge im internen Meldesystem sollten zu Beweis Zwecken entsprechend dokumentiert werden.

Die Einführung solcher interner Meldesysteme wird Unternehmen vor eine Vielzahl von Aufgaben stellen. Hierbei sind insbesondere die Regelungen des Datenschutzes, des Gesellschaftsrechts, des Geschäftsgeheimnisschutzes und des Arbeitsrechts zu nennen.

#### IV. EXTERNE MELDEKANÄLE UND MÖGLICHE OFFENLEGUNG

Wenn ein Unternehmen zwar über einen internen Meldekanal verfügt, der Hinweisgeber jedoch im Falle einer internen Meldung bspw. mit negativen Konsequenzen zu rechnen hat oder die Nutzung des internen Meldewegs zwecklos wäre, so kann sich dieser direkt über einen externen Meldekanal an die zuständige Behörde wenden und unterliegt somit – unter der Maßgabe der Gutgläubigkeit des Hinweisgebers – dem Schutz der Richtlinie.

Falls die interne und/oder externe Meldung eines Hinweisgebers ergebnislos waren oder er Grund zur Annahme hat, dass der Verstoß über den er berichten möchte, eine Gefährdung des öffentlichen Interesses darstellt oder er im Fall einer externen Meldung mit Repressalien zu rechnen hat, so genießt auch ein Hinweisgeber, der sich direkt an die Öffentlichkeit wendet, ebenso den Schutz der Richtlinie, insbesondere den Schutz vor Repressalien.

Ein funktionierendes internes Meldesystem ist somit eine wichtige Voraussetzung, um Hinweise intern behandeln zu können.

#### V. SANKTIONEN

Die Richtlinie verpflichtet die Mitgliedstaaten angemessene und abschreckende Sanktionen für Unternehmen und natürliche Personen festzulegen, welche

- Meldungen behindern,
- Repressalien gegen Hinweisgeber ergreifen,
- mutwillige Gerichtsverfahren gegen den Hinweisgeber anstrengen oder
- die Vertraulichkeit der Identität von Hinweisgebern verletzen.

#### VI. FAZIT

In Anbetracht der Vielzahl der Herausforderungen und Aufgaben, welche die Umsetzung der Richtlinie an Unternehmen stellt, sollten Unternehmen des privaten und des öffentlichen Sektors frühzeitig mit der Konzeption und gegebenenfalls der Implementierung eines angemessenen Hinweisgebersystems beginnen.

Die Experten der Schindhelm Allianz stehen Ihnen für Fragen zur Whistleblower-Richtlinie jederzeit gerne zur Verfügung.

#### KONTAKT

##### **Bulgarien:**

*Cornelia Draganova*  
*Cornelia.Draganova@schindhelm.com*

##### **Deutschland:**

*Henning Kohlmeier*  
*Henning.Kohlmeier@schindhelm.com*

*Karolin Nelles*

*Karolin.Nelles@schindhelm.com*

*Maximilian Oppelt*

*Maximilian.Oppelt@schindhelm.com*

*Sarah Schlösser*

*Sarah.Schloesser@schindhelm.com*



**Italien:**

Debora D'Amico  
Debora.Damico@schindhelm.com

**Österreich:**

Matthias Steyrer  
M.Steyrer@scwp.com

**Polen:**

Katarzyna Gospodarowicz  
Katarzyna.Gospodarowicz@sdzlegal.pl

**Rumänien:**

Helge Schirkonyer  
Helge.Schirkonyer@schindhelm.com

**Spanien:**

Unai Mieza  
U.Mieza@schindhelm.com

**Slowakei:**

Gabriela Janíková  
Janikova@scwp.com

**Tschechien:**

Eva Scheinherrová  
Scheinherrova@scwp.cz

**Türkei:**

Senem Güçlüer  
Senem.Gucluer@schindhelm.com

**Ungarn:**

Beatrix Fakó  
B.Fako@scwp.com