



**Checkliste - Ist Ihr
Unternehmen ausreichend
gegen
Wirtschaftskriminalität
abgesichert?**



**WHISTLEBLOWER
PARTNERS**

Prüfen Sie durch Ankreuzen von 20 Fragen, ob Ihr Unternehmen ausreichend gegen Wirtschaftskriminalität geschützt ist.

Governance und Risikobewertung

1. Wurde das Unternehmen Opfer von Wirtschaftskriminalität, z. B. durch Mitarbeiter, oder hat das Unternehmen selbst gegen Gesetze verstoßen?
2. Bewertet das Unternehmen regelmäßig das Risiko, Opfer von Wirtschaftskriminalität zu werden oder durch Mitarbeiter oder auf andere Weise gegen Vorschriften zu verstoßen?
3. Nimmt das Unternehmen externe rechtliche oder sonstige Beratung in Anspruch, um sicherzustellen, dass das Unternehmen die Gesetzgebung einhält?
4. Aktualisiert das Unternehmen regelmäßig seine Risikobewertung, falls vorhanden?

Berichterstattung an das Management

5. Schließt der externe Prüfer eine Bewertung des internen und externen Betrugsrisikos ein?
6. Verfügt das Unternehmen über eine/n Compliance-Beauftragte/n?
7. Verfügt das Unternehmen über ein Hinweisgebersystem?
8. Gibt es eine benannte Person, die für das Risikomanagement von Wirtschaftskriminalität verantwortlich ist?
9. Verfügt das Unternehmen über Alarmanlagen, Überwachungskameras, Zugangskarten und ähnliche Einrichtungen zur Gewährleistung der physischen Sicherheit?

Politiken und Handbücher

10. Gibt es Politiken, Richtlinien, Geschäftsprozesse oder Verfahren in Bezug auf das Risiko von Wirtschaftskriminalität, einschließlich

- a) Geldwäsche und Terrorismusfinanzierung,
- b) Betrugsprävention,
- c) DSGVO und Datensicherheit,
- d) Bestechung und Korruption,
- e) Verstoß gegen das Wettbewerbsrecht,
- f) finanzielle Sanktionen,
- g) Marktmissbrauch,
- h) Interessenkonflikte und
- i) Dawn-Raid-Handbuch?

11. Werden die Unternehmenspolitiken und -verfahren regelmäßig überprüft?

12. Ergreift das Unternehmen Initiativen, um sicherzustellen, dass das Personal seine Politiken und Verfahren versteht?

13. Stellt das Unternehmen sicher, dass Strategien, Handbücher, Verfahren usw. im gesamten Unternehmen verbreitet und angewendet werden?

Rekrutierung, Überprüfung des Personals, Schulung und Sensibilisierung und Weiterbildung

14. Wird das Personal bei der Einstellung auf relevante Risiken überprüft?

15. Werden die Mitarbeiter über die Risiken der Wirtschaftskriminalität, einschließlich

- a) Geldwäsche und Terrorismusfinanzierung,
- b) Betrugsprävention,
- c) DSGVO und Datensicherheit,
- d) Bestechung und Korruption,
- e) Verstöße gegen das Wettbewerbsrecht,
- f) Finanzsanktionen,
- g) Marktmissbrauch und
- h) Interessenkonflikte informiert,

unterrichtet oder geschult?

16. Hat das Personal Zugang zu Schulungen und Weiterbildungen zu den relevanten Risiken der Wirtschaftskriminalität?

Onboarding von Kunden, Lieferanten, Vertretern, Händlern und anderen Dritten

17. Gibt es Systeme zur Durchführung von Due-Diligence-Prüfungen bei Kunden, Lieferanten, Vertretern, Händlern und anderen Dritten?

18. Werden Due-Diligence-Prüfungen gegenüber Kunden, Lieferanten, Vertretern, Händlern und anderen Dritten auf der Grundlage einer spezifischen Risikobewertung durchgeführt?

19. Werden in einer Beziehung zu Kunden, Lieferanten, Vertretern, Händlern und anderen Dritten fortlaufend Due-Diligence-Prüfungen durchgeführt?

20. Werden die „wirtschaftlich Berechtigten“ bei Kunden, Lieferanten, Vertretern, Händlern und anderen Dritten identifiziert?