

Checkliste

Rolle und Aufgaben der Compliance Funktion

Version 1.0

COMPLIANCE

Gemeinsam. Gestalten.

www.oecov.at

Best Practice | Netzwerk | Diskurs

Der Österreichische Compliance Officer Verbund (ÖCOV) besteht seit November 2013 und fungiert als Interessenvertretung von Personen und Organisationen im Compliance Bereich. Der Verbund besteht aus Mitglieder aus dem Public, Corporate und Bankensektor.

Die wesentlichen Ziele des ÖCOV sind die Förderung der gesetzlichen Stärkung von Compliance-Maßnahmen sowie die Weiterentwicklung des Berufsbildes des Compliance Officer. Erreicht wird dies durch die aktive Teilnahme am öffentlichen und wissenschaftlichen Diskurs, einer Zusammenarbeit mit Interessenvertretungen auf internationaler Ebene und der damit einhergehende Erfahrungsaustausch sowie die Entwicklung von Branchenstandards. Der ÖCOV bietet hierfür eine Plattform für die Vernetzung und den Austausch seiner Mitglieder.

Haftungsfreistellung:

Vorliegende Unterlage soll Ihnen Anregungen für Ihre Arbeit als Compliance Officer bieten und empfehlenswerte Regelungsbereiche aufzeigen. Die Inhalte des Dokuments sind jedoch nicht zur unmittelbaren Übernahme in eigene Regelwerke geeignet. Vielmehr ist es notwendig, Regelungen den jeweils eigenen Erfordernissen, Willen und an die individuell gewünschten rechtlichen Wirkungen anzupassen. Für die konkrete Gestaltung derartiger Regelwerke ist es jedenfalls empfehlenswert, juristische Beratung in Anspruch zu nehmen, sofern in der eigenen Organisation keine juristische Kompetenz vorhanden ist. Es handelt sich bei diesem Dokument jedenfalls um keine Empfehlung des ÖCOV, die Inhalte des Dokuments zu übernehmen, noch übernehmen der ÖCOV, seine Mitglieder und Vertreter in irgendeiner Form eine Haftung für die Verwendung dieser Unterlage. Die Bereitstellung dieses Dokuments soll in der Praxis als Hilfestellung dienen, jedoch ohne Anspruch auf Vollständigkeit oder Richtigkeit zu erheben.

Rolle und Aufgaben der Compliance Funktion

Vorwort

Die Arbeitsgruppe „Organisation“ des „Österreichischer Compliance Officer Verbund (ÖCOV)“ strebt mit beiliegender Ausarbeitung eine Hilfestellung für

- die Compliance Verantwortlichen/Officers
- die Leitung von Organisationen/Unternehmen

in der Rollen- und Aufgabenzuordnung zum Thema Compliance in ihrer Organisation an.

Der Anlass dazu lag in der oft sehr breit angewandten Beschreibung, dass Compliance im Wege einer Generaldefinition für die Bemühungen zur die Einhaltung aller verbindlichen Vorschriften (wie Gesetze) etabliert wird, jedoch die gelebte Praxis zeigt, dass einige Compliance-Funktionen von anderen Organisationseinheiten (üblicherweise Stabstellen) wahrgenommen werden und so mit sich die Compliance-Verantwortlichen nur für einen eingeschränkten Kreis verbindlicher Vorschriften zuständig sehen. Sowohl für die Compliance-Verantwortlichen als auch für die Leitung der Organisation ist eine präzise Rollen- und Aufgabenzuordnung aller Compliance-Aktivitäten in der Organisation von wesentlicher Bedeutung. Dazu sollen die nachstehend beschriebenen Arbeitsbehelfe dienen.

Beschreibung und Verwendung der Beilagen

Folgende Dokumente stehen beiliegend zur Verfügung:

- Check-Liste „Rollen und Aufgaben der Compliance-Funktion“
- Check-Liste „Risikolandkarte“

Beide Listen sind als individuell auf die jeweilige Organisation anzupassender Arbeitsbehelf verstanden.

Die Check-Liste „Rollen und Aufgaben“ beschreibt einzelne Aufgaben, die typischerweise in einer Compliance-Funktion unabhängig von konkreten Risikogebieten auszuführen sind und lehnt sich dabei an gängige Standards an. Für jedes Risikogebiet auf der erforderlichenfalls adaptierten Risikolandkarte, für welches Compliance-Maßnahmen von der Organisation implementiert werden, ist die Liste „Rollen und Aufgaben“ mit der für die jeweilige Aufgabe zuständigen Unternehmenseinheit zu befüllen. Allenfalls können auch noch weitere Aufgaben ergänzt werden.

Die Check-Liste „Risikolandkarte“ stellt auf die Organisation möglicherweise zur Anwendung kommende Risiken dar und ist ebenfalls individuell anzupassen. Diese Liste dient der Konkretisierung der vorgenannten Check-Liste „Rollen und Aufgaben“. Neben der Aufgaben- und Rollenbeschreibung kann diese Liste auch als Hilfestellung für die Compliance-Risikoanalyse herangezogen werden.

Rolle und Aufgaben der Compliance-Funktion der [Organisation]: [Risikogebiet ¹]				
	Aufgabenstellung	verantwortlich ²	Mitwirkung ³	Kommentar
1	Design/Beschreibung/Dokumentation des CMS			
1.1	Erhebung der Rahmenbedingungen			gesetzl. Erfordernisse, organisator. Gegebenheiten
1.2	Vorschlag			
1.3	Entscheidung			
1.4	Umsetzung			
1.5	Kommunikation			
2	Risikoanalyse			
2.1	Prozess: Vorschlag (wie, wer)			
2.2	Prozess: Entscheidung			
2.3	Identifikation relevanter (Geschäfts)Vorgänge			
2.4	Compliance-Risiken: Bewertung,			
2.5	Priorisierung			
2.6	Dokumentation und Bericht an die Leitung			
2.7	Formelle Entscheidung			
2.8	Review der Analyse [jährlich]			
3	Handlungsanweisungen			Richtlinien, Guidelines, wie z.B. Geschenke, Einladungen
3.1	Entwurf			
3.2	Formelle Entscheidung			
3.3	Kommunikation			
3.4	Help Desk			
4	Besetzung von Schlüsselpositionen			
4.1	Vorschlag der Definition			
4.2	Formelle Entscheidung			

1 Je ein Chart pro Risikogebiet. Zu den Risikogebieten siehe separate Risikolandschaft

2 Federführung/Durchführung,

3 Mitentscheidung, Mitarbeit/Unterstützung, Informationsbeistellung

4.3	Compliance Risiko-Bewertung (vor Besetzung)			
4.4	Entscheidung über Besetzung			
5	Training			
5.1	Trainingsplan Vorschlag			
5.2	Trainingsplan Entscheidung			
5.3	Festlegung Methode, Dauer und Inhalt			
5.4	Festlegung Teilnehmer			
5.5	Einladung Teilnehmer			
5.6	Organisation der Infrastruktur			
5.7	Trainer			
5.8	Dokumentation (Teilnehmer, Zeitpunkt, Dauer, Inhalt)			
6	Überwachungsaudits			
6.1	Audit-Plan Vorschlag			
6.2	Audit-Plan Entscheidung			
6.3	Ad-hoc Audit Vorschlag			
6.4	Ad-hoc Audit Entscheidung			
6.5	Durchführung Audit			
6.6	Berichterstattung durch ...			
6.7	Berichterstattung an ...			
6.8	Vorschlag Verbesserungsmaßnahmen			
6.9	Entscheidung Verbesserungsmaßnahmen			
6.10	Durchführung Verbesserungsmaßnahmen			
6.11	Festlegung einer Überprüfung des CMS (angemessen, geeignet, wirksam?)			
6.12	Durchführung der Überprüfung des CMS			
6.13	Entscheidung über Verbesserungsmaßnahmen			
6.14	Umsetzung von Verbesserungsmaßnahmen			
7	Laufende Kontrollen			
7.1	Control Design: Vorschlag			
7.2	Control Design Entscheidung			
7.3	Durchführung Kontrolle			

7.4	Berichterstattung durch ...			
7.5	Berichterstattung an ...			
7.6	Vorschlag Verbesserungsmaßnahmen			
7.7	Entscheidung Verbesserungsmaßnahmen			
7.8	Durchführung Verbesserungsmaßnahmen			
8	Hinweisgebersystem			
8.1	Vorschlag zur Methode			IT-Lösung, Ombudsperson,...
8.2	Entscheidung zur Methode			
8.3	Implementierung des Systems			
8.4	Kommunikation			
8.5	Verwaltung (Doku) von Meldungen			
8.6	Bewertung von Meldungen			
8.7	Entscheidung über die konkrete Behandlung von Meldungen			
8.8	Untersuchung des gemeldeten Sachverhalts			
8.9	Bewertung des gemeldeten Sachverhalts			
8.10	Entscheidung über Maßnahmen			(siehe oben zu „Überwachung“ und unten zu „Disziplinarmaßnahmen“)
8.11	Datenschutzverfahren			
8.12	Betriebsvereinbarung			
9	Disziplinarmaßnahmen			
9.1	Regelung: Vorschlag			Maßnahmen, Entscheidungsprozess
9.2	Regelung: Entscheidung			
9.3	Regelung: Kommunikation			
9.4	Vorschlag Disziplinar-Maßnahmen			
9.5	Entscheidung Disziplinar-Maßnahmen			
9.6	Durchführung Disziplinar-Maßnahmen			
10	Regel-Compliance-Kommunikation			
10.1	Vorschlag (was, wann, wie)			
10.2	Entscheidung			
10.3	Durchführung			
10.4	Bericht an Geschäftsleitung			

10.5	Bericht an AR			
11	Krisen-Compliance-Kommunikation			
11.1	Vorschlag (was, wann, wie)			
11.2	Entscheidung			
11.3	Durchführung			
12	Business Partner (BP) Check			
12.1	Prozess: Vorschlag			
12.2	Prozess: Entscheidung			
12.3	Durchführung des BP Check			
12.4	Entscheidung über BP			
13	M&A Compliance Due Diligence			
14	Abwicklung von Behörden-/Gerichtsverfahren			ggfls.einschl.Hausdurchsuchung
15	Einschaltung externer Berater/Vertreter			
15.1	Vorschlag			
15.2	Entscheidung			
15.3	Abwicklung			

Risikogebiete	Gesetze sowie interne Regelungen (bspw. Interessenkonflikte; Code of Conduct)	Risiko (Identifizierte Risikobereiche bspw. Finanzen, Personal, Einkauf, Kapitalmarkt, Datenschutz)	Operative Zuständigkeit	Risikoträger
Verwaltungsstrafrecht	VStG	Verantwortlichkeit der Geschäftsleitung (oder § 9 VStG Verantwortlicher) nach dem VStG für Strafen nach div. Verwaltungsgesetzen		
Unternehmensstrafrecht	VbVG	<p>Strafrechtliche Verantwortlichkeit für strafbare Handlungen von Entscheidungen bzw. Mitarbeitern.</p> <p><u>Compliance Risiko im engeren Sinn:</u> keine hinreichenden checks and balances keine hinreichenden technischen und organisatorischen sowie personellen Maßnahmen zur Verhinderung solcher Taten.</p>		
Amtshaftung	AmtshaftungG	sonstige Körperschaften des öffentlichen Rechts (Rechtsträger) haften nach den Bestimmungen des bürgerlichen Rechts für den Schaden am Vermögen oder an der Person, den die als ihre Organe handelnden Personen in Vollziehung der Gesetze durch ein rechtswidriges Verhalten wem immer schuldhaft zugefügt haben		

<p>Wirtschaftsstrafrecht</p>	<p><u>Strafgesetzbuch, insbesondere nachstehende Bestimmungen:</u> Betrug, Untreue, Gläubigerschutzdelikte, Erpressung, Diebstahl, Veruntreuung, Computerstrafrechtsdelikte (118a, 119, 126a StGB, 51 DSG), Geldwäscherei, Umweltstrafrecht, Privatspäre und Geheimnisverletzungen (122-124), Zuverlässigkeit von Urkunden und Beweiszeichen (223, 229), Ehre und Rechtspflege (111, 152, 297) Geschenkannahme durch Machthaber, § 165 Geldwäscherei, § 168b wettbewerbsbeschränkende Absprachen bei Vergabeverfahren, § 148 schwerer Betrug sowie § 148 gewerbsmäßiger Betrug auf grund von Absprachen.</p>	<p><u>Untreue - Beispiele:</u> Einkauf von Waren zu überhöhten Preisen (um Geld aus dem Unternehmen zu bringen; Kickback, um für sich selbst Vorteil zu erlangen). Bezahlung fingierter Rechnungen (um Geld aus dem Unternehmen zu bringen). Gestaltung von Ausschreibungen/Spezifikationen, damit ein bestimmter Lieferant zum Zug kommt (um für sich selbst einen Vorteil zu erlangen). Falsche Klassifizierung/Kontierung/Buchung von Kosten für Events, Sponsoring, Beratung oder Spesen etc. um Freigabe prozesse zu umgehen oder die Grundlage für Zahlungen zu verschleiern und Spielraum für unrechtmäßige Verwendung zu schaffen. Zahlungen auf Aufforderung des Lieferanten an Dritte, in Bar, in andere Länder als den Firmensitz oder auf Nummernkonten (neben Korruption auch Geldwäschereirisiko). <u>Compliance-Risiko im engeren Sinn:</u> nicht ausreichend spezifizierte, praktikable, den Mitarbeitern bekannte Richtlinien; Abläufe nicht praktikabel, bekannt, angemessen (4-Augen, etc) Keine ausreichende Sensibilisierung von Mitarbeitern und insb. Führungskräften für Korruptionsrisiken (z.b. Erkennen von auffälligen Verhaltensweisen, Thematisierung in Arbeitsbesprechungen).</p>		
------------------------------	---	--	--	--

<p>Anti-Korruptionsstrafrecht</p>	<p><u>Strafgesetzbuch, insbesondere nachstehende Bestimmungen:</u> § 304 Bestechlichkeit, § 305 Vorteilsannahme, § 306 Vorteilsannahme zur Beeinflussung, § 307 Bestechung, § 307a Vorteilszuwendung, § 307b Vorteilszuwendung zur Beeinflussung, § 308 Verbotene Intervention. § 309 Geschenkkannahme und Bestechung von Bediensteten oder Beauftragten FCPA/UK Bribery Act <u>Interne Regelung:</u> SpendenRL, GeschenkeRL, Code of Conduct</p>	<p><u>Korruption - Beispiele:</u> Um einen Auftrag zu erlangen, wird vom Kunden die Beauftragung eines bestimmten Partners gefordert. Amtsträger verlangt eine gesetzlich nicht festgelegte Gebühr für die positive Erledigung eines Antrages. Geschenke/Einladungen, welche als Bestechung gewertet werden können (um eine Entscheidung zugunsten des Vorteilsgebers zu erwirken oder nur "Klimapflege" zu betreiben). <u>Compliance-Risiko im engeren Sinn:</u> nicht ausreichend spezifizierte, praktikable, den Mitarbeitern bekannte Richtlinien; Abläufe nicht praktikabel, bekannt, angemessen (4-Augen, etc) Keine ausreichende Sensibilisierung von Mitarbeitern und insb. Führungskräften für Korruptionsrisiken (z.b. Erkennen von auffälligen Verhaltensweisen, Thematisierung in Arbeitsbesprechungen). <u>Beispiel FCPA:</u> Bestechung eines ausländischen Amtsträgers <u>Compliance-Risiko im engeren Sinn:</u> kein ausreichendes CMS iSd FCPA Guides oder UK Bribery Act</p>		
<p>Einkauf</p>	<p>Bundesvergabegesetz; Strafrecht <u>interne Richtlinien:</u> RL zur Geschäftspartnerprüfung</p>	<p><u>Verstoß gegen Ausschreibungsbestimmungen - Beispiele:</u> Gestaltung von Ausschreibungen/Spezifikationen, damit ein bestimmter Lieferant zum Zug kommt (um für sich selbst einen Vorteil zu erlangen).</p>		

Wettbewerb	<p>UWG, insbesondere nachstehende Bestimmungen:</p> <p>§ 10 UWG Bestechung von Bediensteten oder Beauftragten (ev. im Fall von Beteiligungen unter 50 %)</p>			
Kartellrecht	UWG	<p>Unzulässige Absprachen mit Mitbewerbern (Preisabsprachen, Konditionenabsprachen, Marktaufteilung, Austausch wettbewerbsrelevanter Informationen wie zb. Produktionskosten, Kundendateien, Umsätze, Marketingpläne etc.) Missbrauch einer Marktbeherrschenden Stellung (Behinderung Mitbewerber, unsachliche Ungleichbehandlung von Kunden/Lieferanten, unverhältnismäßige Rabatte, unsachlicher Ausschluss einzelner Lieferanten, Compliance-Risiken im engeren Sinn: Keine ausreichenden internen Richtlinien; keine ausreichende Einbindung der Compliance/Recht.</p>		

Insidercompliance	<p>Börsegesetz, insbesondere die Bestimmungen:</p> <p>48b ff</p> <p><u>Interne Regelung: InsiderRL</u></p>	<p>Verwertung, Empfehlung, Weitergabe hinsichtlich Insiderinformation als Kapitalmarktbezogener Insider (auch innerhalb des Konzerns bzw. des Unternehmens).</p> <p>Verletzung von Organisationspflichten (Vertraulichkeitsbereiche),</p> <p>Ermöglichung der Möglichkeit für Dritte, Insiderinformationen zu erlangen.</p> <p><u>Compliance-Risiken im engeren Sinn:</u></p> <p>Prüfung der Einhaltung der KapitalmarktRL, Mitarbeiterschulungen,</p>		
Öffentlichkeitsarbeit	Medienkooperations- und Medienförderungstransparenzgesetz	Nichtmeldung von Inseraten, Eigenwerbung		

<p>Personal Arbeits- und Sozialrecht</p>	<p>Arbeitsverfassungsg, ArbeitszeitG, MutterschutzG, Behinderteneinstellungsg, Ausländerbeschäftigungsg, ASVG, EStG, ArbeitslosenversicherungG, Gleichbehandlungsg, AngestelltenG, ArbeitsinspektionsG, Arbeitsvertragsrechts- anpassungsg, Maschinensicherheits- verordnung, Sicherheitsvertrauenspersonen- verordnung, Arbeitsmittelverordnung, Grenzwerteverordnung (? Produktion Münze, OeBS?) Lebensmittelrecht (Kantine?) <u>Interne Richtlinien</u>: RL zu Nebenbeschäftigung</p>	<p><u>Beispiele</u>: Verletzung von Bestimmungen hinsichtlich Arbeitszeit, Entgelt, Sozialversicherung- und Lohnsteuer, Mutterschutz, Behindertenschutz, Ausländerbeschäftigung, Persönlichkeitsschutz, Mitarbeiterüberwachung, Arbeitnehmerschutz/Sicherheit (z.b. Durchführung einer Gefahrenanalyse), etc. <u>Compliance im engeren Sinn</u>: keine ausreichenden Maßnahmen zum Schutz von Schädigungen von Gesundheit und Eigentum von Mitarbeitern --> VbVB</p>	<p>bspw.: Personalabteilung</p>	
--	--	---	-------------------------------------	--

Datenschutz	Datenschutzgesetz und IT-Sicherheit	<p>Rechtswidrige Verarbeitung von personenbezogenen Daten, wenn dafür keine ausreichende rechtliche Erlaubnis vorliegt. Erhebung von mehr Daten, als benötigt werden. Nichteinhaltung der Zweckbindung bei der Verarbeitung von personenbezogenen Daten. Transparenz. Beachtung der Pflichten gegenüber der Datenschutzbehörde. Ausreichende Absicherung der Datenverarbeitung. Unterlassung von Löschung von Daten, für die keine Erlaubnis vorliegt. Schutz von Geschäfts- und Betriebsgeheimnissen</p> <p>Ungenügende Sicherung von Daten (Infrastruktur etc.)</p> <p><u>Compliance-Risiken im engeren Sinn:</u> Ausreichende Regelungen.</p>		
Umweltrecht	Verwaltungsstrafrecht, GewerbeO, Abfallwirtschaftsgesetz, Bundesgesetz über Umweltschutz, ElektrogeräteVO, VerpackungsVO, ChemikalienG, UmweltmanagementG, Div. Gewerberechtliche Vorschriften/VO	Verletzung von Rechtsvorschriftenkein ausreichendes internes Kontrollsystem		

Geistiges Eigentum	Intellectual Property (EDV, Geldproduktion?): MarkenschutzG, MusterschutzG, PatentG, UrheberrechtsG,	Verletzung von fremden Schutzrechten		
Gesellschaftsrecht	Gesellschaftsrecht (UGB, AktG, Finanzstrafgesetz etc.)	strafrechtlich relevante Verletzung von Accountingrules Verantwortung der Aufsichtsräte? IKS, RM, Berichtspflichten etc. --> Corporate Governance		
Zivilrecht	ABGB	Sachen, und Schuldrecht, insb. Gestaltung von Verträgen sowie vertragliche/deliktsische Ersatzpflichten		
Konsumentenschutz	ABGB; KSchG			

Gewerberecht	GewerbeO	Gewerbeberechtigungen		
Produktsicherheit	<ul style="list-style-type: none"> • PSG (Produktsicherheitsgesetz) • LMSVG (Lebensmittelsicherheits- und Verbraucherschutzgesetz) • Verordnung (EG) Nr. 178/2002 ("General Food Law") • Weiterführende Verordnungen wie z.B. zur Spielzeugsicherheit 	<ul style="list-style-type: none"> • Verantwortlichkeit (Verantwortlich Beauftragter) nur nachweislich sichere Produkte in Verkehr zu bringen bzw. nicht sichere Produkte aus dem Verkauf zu nehmen oder öffentlich zurückzurufen • Erfüllung der Sorgfaltspflicht durch Kontrolle und Überprüfung der Produkte vor der In-Verkehr-Bringung • Verwaltungsrechtliche Strafbarkeit bei In-Verkehr-Bringung von Produkten mit z.B.: irreführenden Angaben, wertgeminderter Zusammensetzung, Kennzeichnungsfehlern • Straftatbestand bei vorsätzlicher oder fahrlässiger In-Verkehr-Bringung von z.B. gesundheitsschädlichen Lebensmitteln 		
Aufsichtsrecht	BWG, WAG, VAG, BörseG; InvFG; SparkassenG; DepotG;Verordnungen; europarechtliche Vorschriften insbes. Verordnungen; ESMA und EBA Vorschriften; FMA Rundschreiben; E-Control; branchenübliche Regulierungen (GlücksspielG);			
Steuerrecht				
Finanzstrafrecht	Bewertungsvorschriften;			

Geldwäsche und Sanktionen				
Social Compliance	CSR			
Code Of Conduct/Ethische Grundsätze				
interne Richtlinien		Mangement d. Richtlinien		
Internationale Standards				