Compliance

Interne KC-Richtlinie

Version: 0.1
Datum: 20-Nov-2024

Dokumentenhistorie

Dokument: Compliance
Version: 0.1
Status: Draft
Projekt: Compliance
Dateiname: Compliance - draft
Autor: KuglerConsulting GmbH

Datum	Seite	Änderung	Autor
23-Apr-2024		Initiale Erstellung	JM

Freigabe

Firma	Name	Datum	Unterschrift
KuglerConsulting GmbH	Steffen Kugler		

Mit der Freigabe dieser Version des Dokuments wird dieses gültig. Alle vorherigen Versionen desselben Dokuments verlieren hierdurch ihre Gültigkeit.

Kommentiert [JM1]: Keine rückwirkende Geltung des Dokuments.

Ausdrucke unterliegen keiner Änderungsverfolgung

Ersteller

KuglerConsulting GmbH
Im Beundle 14
D-71540 Murrhardt

Telefon: +49 (0) 7192 9332-0
Telefax : +49 (0) 7192 9332-10

Urheberrecht

Inhalt

1 Abbildungsverzeichnis 5

2 Abkürzungsverzeichnis 6

3 Einleitung 7

3.1 Sensibilisierung und Schulung / Einführung 7

3.2 Geltungsbereich 7

3.3 Maßnahmen bei Verstößen 8

3.4 Kontakt 8

4 Vorteile für die KuglerConsulting GmbH 9

5 Einladungen, Geschenke, persönliche Vorteile 10

5.1 [Kapitel 7.1] 10

6 Marktbegleiter/Mitbewerber 11

6.1 Eigentum & Vermögenswerte 11

6.2 [Kapitel 7.1] 11

7 Compliance bei der KuglerConsulting GmbH 12

7.1 [Kapitel 7.1] 12

8 Lieferanten und Lieferketten 13

9 Schutz und Sicherheit (Informationen/Daten/Vermögen) 14

10 Offizielle Organe (Behörden) 15

10.1 [Kapitel 7.1] 15

11 Verhaltenskodex / Code of Conduct 16

12 Gesetze, Richtlinien und Vorschriften 17

13 Normen und Standards 19

13.1 [Kapitel 7.1] 19

14 Entscheidungshilfe 20

15 Notizen, Anmerkungen, Tipps, Links (temporär) 21

1 Abbildungsverzeichnis

Abbildung 1: Beispiel-Abbildung 8

2 Abkürzungsverzeichnis

AG	Auftraggeber
AGG	Allgemeines Gleichstellungsgesetz
AN	Auftragnehmer
CI	Corporate Identity
CoC	Code of Conduct / Verhaltenskodex
DSGVO	Datenschutz-Grundverordnung
KC	KuglerConsulting GmbH
KVP	Kontinuierlicher Verbesserungsprozess
PDF	Portable Document Format. Plattformunabhängiges Dateiformat von Adobe Systems.
PSA	Persönliche Schutzausrüstung
ANÜ	Arbeitnehmerüberlassung
LAN	Local Area Network – lokales Rechnernetz
WLAN	Wireless Local Area Netzwork – lokales Funknetz (in de rRegel nach Standard der IEEE-802.11-Familie)
IEEE	Institute of Electrical and Electronics Engineers - weltweiter Berufsverband von Ingenieuren, Technikern, Wissenschaftlern und angrenzender Berufe
IT	Informationstechnologie
DIN	Deutsches Institut für Normung
EN	Europäische Norm
ISO	International Organization for Standardization – Internationale Organisation für Normung
KI	Künstliche Intelligenz
DGUV	Deutsche gesetzliche Unfallversicherung
[Abkürzung]	[Erläuterung]

3 Einleitung

[…]

- Compliance = Regeltreue von Unternehmen und ihren Mitarbeitern
- Verpflichtung des Unternehmens, Gesetze, Vorgaben und Vorschriften einzuhalten.
- Verpflichtung des Unternehmens, unternehmensinterne Richtlinien und Vorschriften einzuhalten.
- "Compliance bedeutet, dass sich ein Unternehmen an die geltenden Regeln und Gesetze hält - sowohl landesspezifische Gesetze als auch Vorgaben von Regulierungsbehörden und interne Weisungen im Unternehmen."
- Einführung einer Compliance-Richtlinie durch die Geschäftsführung (Kommunikation / Schulung der Mitarbeitenden).
- Compliance-Verstöße können strafrechtliche Folgen (für das Unternehmen) haben.

3.1 Sensibilisierung und Schulung / Einführung

[…]

- KC-Mitarbeitende werden für die Themen sensibilisiert
- Schulungen?
- Vorgehen / Einführung:
  - Inhalte definieren. Als Erstes müssen die Verantwortlichen die Regeln, Richtlinien und Werte des Unternehmens erarbeiten. ...
  - Ergebnisse ausformulieren. ...
  - Juristische Prüfung. ...
  - Das Dokument allen Mitarbeitern zur Verfügung stellen. ...
  - Schulungen. ...
  - Regelmäßig prüfen und aktualisieren / Auffrischungs-Schulungen.
- Bei Bedarf werdne Übersetzungen des KC-Codes of Conduct angestrebt, um dem relevanten Personenkreis ein passendes (Nachschlage-)Werk zur Verfügung stellen zu können.
  Im Zweifelsfall oder bei Abweichungen hat die deutschsprachige Variante Vorrang.
- Bei Unsicherheiten ist die jeweilige Führungsperson Ansprechpartner bzgl. des Codes of Conduct.
- …

3.2 Geltungsbereich

[…]

- Leitlinie für die Mitarbeiter, an der sie sich am Arbeitsplatz und im Umgang mit Geschäftspartnern orientieren können
- Geschäftspartner und Arbeiter/Partner die im Namen von KC arbeiten zur Einhaltung des Code of Conduct anhalten? → Vertragsbestandteil mit Lieferanten (kaskadierendes System auf Sub-Lieferanten)
- Geltungsbereich definieren (alle Mitarbeiter und alle Personen, die Funktionen in Namen des Unternehmens (KC) ausüben)

- Compliance ist auch für alle Geschäftspartner, Zulieferer, etc. verpflichtend (Ist dies durchsetzbar?).
- Bzgl. Nachhaltigkeit und Umweltschutz zumindest im Rahmen der gesetzlichen Vorgaben und im Rahmen des Möglichen und Zumutbaren.
  KC behält sich vor, Prüfungen bzgl. relevanter Bereiche bei Geschäftspartnern durchzuführen. Dies kann u.a. in Form einer Selbstauskunft des Geschäftspartners oder vor Ort erfolgen. Vor-Ort-Überprüfungen erfolgen nach Vorankündigung und im Beisein des Geschäftspartners während regulärer Geschäftszeiten sowie unter Einhaltung geltender Gesetze und Vorschriften und unter Berücksichtigung des Datenschutzes.
- …

Abbildung 1: Beispiel-Abbildung

3.3 Maßnahmen bei Verstößen

[…]

- Handlungsmöglichkeiten der Mitarbeitenden bei Verstößen
- Verstöße gegen Compliance werden bei KC nicht toleriert.
- Das Nicht-Einhalten von Compliance oder seiner Teile wird als (Regel-)Verstoß gewertet.

3.4 Kontakt

[…]

- Die jeweilige Führungsperson
- Zentrale Compliance-Stelle / zentraler Compliance-Beauftragter/Compliance-Officer
- E-Mail: compliance@kuglerconsulting.com

Kommentiert [JM2]: Postfach einrichten?

4 Vorteile für die KuglerConsulting GmbH

[…]

- Vermeiden und Minimieren von Risiken
- Schutz vor Nachteilen (Haftung, Reputation, Abmahnungen, etc.)
- Vereinheitlichung innerhalb von KC
- Vermeiden von zivilrechtlichen und strafrechtlichen Risiken
- Frühzeitiges Erkennen und Vermeiden von Risiken
- Vermeiden/Verringern der Haftung von Geschäftsführung (und Vorstand)
- …

5 Einladungen, Geschenke, persönliche Vorteile

[…]

- Einladungen
  - Welche Einladungen dürfen angenommen werden?
- Geschenke
  - Welche Geschenke dürfen angenommen werden?
- Persönliche Vorteile
  - Umgang mit dem Thema?
- Sonstige Werte für Arbeit bei KC
  - Gegenseitiger Respekt und Wertschätzung
  - Gegenseitige Achtung
- Einhalten der KC-Richtlinien
- …

5.1 [Kapitel 7.1]

[…]

6 Marktbegleiter/Mitbewerber

[…]

- Verhalten ggf. Marktbegleitern/Mitbewerbern
- Know-How-Schutz
- Respektieren und Achten von Eigentum, Marken, etc.
- …

6.1 Eigentum & Vermögenswerte

[…]

- Geistiges Eigentum
  - Respektieren der Rechte an geistigem Eigentum
  - Schutz entsprechender Daten
- Rechte Dritter:
  - Das (geistige) Eigentum von Geschäftspartnern und sonstigen Dritten wird anerkannt und respektiert.
  - Achten und Anerkennen von Patenten, Geschäfts- und Betriebsgeheimnissen
- …

6.2 [Kapitel 7.1]

[…]

7 Compliance bei der KuglerConsulting GmbH

[…]

- Siehe dieses Dokument
- Weiterführende Vereinbarungen und Regelungen: siehe Code of Conduct der KuglerConsulting GmbH
- …

7.1 [Kapitel 7.1]

[…]

8 Lieferanten und Lieferketten

[…]

- Prüfung auf KC-relevante Themen

9 Schutz und Sicherheit (Informationen/Daten/Vermögen)

[…]

- Siehe Code of Conduct der KuglerConsulting GmbH

10 Offizielle Organe (Behörden)

[…]

- Siehe auch Code of Conduct der KuglerConsulting GmbHd
- Gesetze und Vorschriften einhalten
    - Einhalten von Gesetzen und Vorschriften (z.B. Datenschutz, Korruption, Umweltschutz)
    - Geltende rechtliche Verbote, Gebote und Pflichten werden jederzeit beachtet.
- Buchführung, Bilanzen, etc. (siehe auch Kap. 5)
- Strafverfolgung?
- Steuern, Zölle, Abgaben
- Erteilen von Auskünften
    - Befugten Stellen werden Auskünfte bei gerechtfertigten Anfragen erteilt.
- Einhalten von jeweils geltenden Steuer- und Zollvorgaben und Vorschriften.

10.1 [Kapitel 7.1]

[…]

11 Verhaltenskodex / Code of Conduct

Siehe KC-Richtlinie zu Code of Conduct / Verhaltenskodex der KuglerConsulting GmbH.

12 Gesetze, Richtlinien und Vorschriften

[…]
Beispiele für Gesetze, Normen, Richtlinien und Vorschriften:

- Datenschutz-Grundverordnung (DSGVO / GDPR)
- Lieferkettengesetz
- Arbeitszeitgesetz
- Rechtliche Rahmenbedingungen für SaaS (Software as a Service)?
- Bundesdatenschutzgesetz (BDSG, BDSchG)
- Landesdatenschutzgesetz (LDSG)
- Telekommunikationsgesetz (TKG)
- Handelsgesetzbuch in Verbindung mit den Grundsätzen ordnungsgemäßer Buchführung (GoB) (HGB)
- Standards des Instituts der Wirtschaftsprüfer (IDW)
- Vorschriften bzgl. Buchhaltung, Bilanzen, etc.?
- Urheberrecht (z.B. bzgl. Drittkomponenten, Lizenzen, etc.)
- Einhaltung sämtlicher Verträge/Vereinbarungen mit Partnern, Lieferanten, Kunden, etc.
- Markenrecht / Wettbewerbsrecht (keine Bestechung, keine Annahme von Geschenken, etc.)
- Software- und Lizenzverträge bzw. -vereinbarungen:
- https://www.ihk.de/stuttgart/fuer-unternehmen/recht-und-steuern/it-recht/ueberlassung-von-standardsoftware-das-sind-die-regeln-4368114
- Handelsgesetzbuch (HGB)
- gegebenenfalls IFRS/IAS (internationale Rechnungslegung), BilMoG (Bilanzrechtsmodernisierungs-Gesetz)
- GoB und GoBS (Grundsätze ordnungsgemäßer Buchführung/Buchführungssysteme)
- Rundschreiben und Standards des Instituts der deutschen Wirtschaftsprüfer, zum Beispiel IDW FAIT I, II und III
- digitale Betriebsprüfung (GdPDU)
- Umsatzsteuergesetz (UStG) - Paragraf 14 UStG (Aufbewahrung von Rechnungen
- Urhebergesetz (UrhG)
- Dokumentationspflichten
- KC-interne Richtlinien (I:\Anleitungen und Richtlinien)
- Geschäftsgeheimnisgesetz (GeschGehG)
- Verhalten am Arbeitsplatz, Verhalten ggü. Externen (Gesetze, Vorschriften & KC-Richtlinien)
- Code of Conduct / Verhaltenskodex bei KC (als Teil der Compliance)
- Arbeitssicherheitsgesetz (ASiG) (z.B. Fluchtwege im Büro und deren Auszeichnung)
- Deutsche Gesetzliche Unfallverhütung (DGUV) - Unfallverhütung
- Allgemeines Gleichbehandlungsgesetz (AGG)
- Gesundheit und Sicherheit am Arbeitsplatz
- Abwesenheiten, Urlaub, etc. --> siehe bestehende KC-Richtlinien

Auf Relevanz für KC zu prüfen:

- Deutscher Corporate Governance Kodex (DCGK) (gilt für börsennotierte Unternehmen)
- Mindestanforderungen an das Risikomanagement? (MaRisk)
- Abgabenordnung
- Signaturgesetz (SigG)

- elektronisches Handels- und Genossenschaftsregister (Ehug)
- Produkthaftungsgesetz (KC-WMS als Produkt)
- Lieferkettengesetz (LkSG) - Gilt seit 01-Jan-2024 für Firmen mit mehr als 1.000 Mitarbeitenden
- Kann für KC relevant werden, wenn Kunden-Unternehmen entsprechender Größe unter das LkSG fallen
- und ihre Lieferanten ebenfalls zur Einhaltung verpflichten (sofern auf Produkte und Dienstleistungen
- von KC anwendbar).
- Corporate Sustainability Due Diligence Directive, CSDDD

13 Normen und Standards

[…]

- Über gesetzliche Vorgaben hinausgehend, wird die Einhaltung der folgenden Normen, Standards bzw. Richtlinien angestrebt.
  - ISO 9001 (Qualität)
  - DIN EN ISO 14001 (Umweltschutz)
  - ISO 45001 (Arbeitsschutzmanagementsystem)
  - Konventionen der internationalen Arbeitsorganisaion (ILO)?
  - DGUV-Vorschriften
- Normen, Standards und Richtlinien, welche nicht gesetztlich/rechlicht verpflichtend sind, aber eingehalten werden sollten (soweit auf KC zutreffend):
  - ISO 9001 - Qualitätsmanagementnorm
  - ISO 9126 - Softwarequalität
  - ISO 25000ff. - Software-Projekte & Software-Qualität
  - ISO 19770 - IT-Asset-Management (Verwalten des IT-Vermögens)
  - ISO 9241 - Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten
  - ISO 45001 - Gesundheitsschutz am Arbeitsplatz
  - IEC 82079 - Dokumentation
  - DIN 5008 - Schreib- und Gestaltungsregeln für die Text- und Informationsverarbeitung
  - ITIL (IT Infrastructure Library) - Best-Practices für die Erbringung von IT-Services - ITIL und/oder DevOps?
  - COBIT (Control Objectives for Information and Related Technology) - Gliederung der Aufgaben der IT in Prozesse undZiele/Steuerungsvorgaben
  - ISO 37301 - Compliance-Management-Systeme
  - ISO 31000 - Risikomanagement
  - ISO 37001 - Anti-Korruptions-Management (Korruptionsbekämpfung)
- …

13.1 [Kapitel 7.1]

[…]

14 Entscheidungshilfe

[…]

1. Fachlich: Habe ich bei meiner Entscheidung alle relevanten Punkte und Belange berücksichtigt?
2. Legal: Bewege ich mich im Rahmen der gesetzlichen und internen Vorgaben und im Rahmen meiner Befugnisse?
3. Vorgesetzte: Kann ich zu meiner Entscheidung stehen, wenn diese anderen Stellen oder öffentlich bekannt wird?
4. Verallgemeinerung: Ist es in Ordnung, wenn in anderen, vergleichbaren Fällen genauso entschieden wird (auch z.B. durch andere Stellen)?
5. Öffentlichkeit: Kann ich meine Entscheidungen auch in der Öffentlichkeit vertreten?
6. Betroffenheit: Könnte ich meine Entscheidung auch als davon betroffene Person akzeptieren?
7. Zweite Meinung: Was würden nahestehende Personen (z.B. Freunde, Familie, Kollegen) zu der Entscheidung sagen?

Habe ich Zweifel, oder kann ich nicht alle Fragen eindeutig mit ‚ja' beantworten, so wende ich mich an meine Führungskraft bzw. die zuständige Stelle.

15 Notizen, Anmerkungen, Tipps, Links (temporär)

Code of Conduct (Verhaltenscodex)

Beispiele:
- Audi: https://www.audi.com/de/sustainability/ethical-leadership/documents-policies.html
- Wikipedia: https://de.wikipedia.org/wiki/Verhaltenskodex

Vorgehen:

1. Inhalte definieren. Als Erstes müssen die Verantwortlichen die Regeln, Richtlinien und Werte des Unternehmens erarbeiten. ...
2. Ergebnisse ausformulieren. ...
3. Juristische Prüfung. ...
4. Das Dokument allen Mitarbeitern zur Verfügung stellen. ...
5. Schulungen. ...
6. Regelmäßig prüfen und ändern.

Laut Hans-Böckler-Stiftung:
„Diese Verhaltensregeln – neudeutsch Codes of Conduct – **unterliegen der Mitbestimmung des Betriebsrates** und gehen über das Weisungsrecht des Arbeitgebers hinaus."
https://www.boeckler.de/de/magazin-mitbestimmung-2744-das-arbeitsrecht-gehoert-zur-compliance-5267.htm, Stand 25-Apr-2024

Audi:
„Für ein funktionierendes […]system sind eine genau geregelte Ablauforganisation, definierte Prozesse, geschulte Mitarbeitende sowie regelmäßige Kontrollen und Audits notwendig. Neben dem Feedback von Auditor_innen und Mitarbeitenden stellen Kennzahlen den wichtigsten Baustein zur Kontrolle der Umweltleistung dar."

Umwelterklärung Niederlassung Neckarsulm, Stand 25-Apr-2024

Anmerkungen:
- Compliance als permanentes Programm (ggf. iterative Bewertung) und nicht als einzelnes Projekt mit definiertem Ende betrachten.
- Siehe auch: I:\Normen und Gesetze
- Risikomanagement etablieren
- Zugänge bei KC (z.B. Risiko, dass Externe Zugang zu Servern/Serverräumen bekommen)
- Fluchtwege, Erste-Hilfe, Verbandbuch
- Professioneller Umgang mit Geschenken --> Richtlinie dient der Reduktion des passiven und aktiven Korruptionsrisikos

  Unterscheidung von Geschenken (= Gegenstände), Zuwendungen (= Vorteile) und Bewirtung (= Mahlzeiten & Spesen), Sonstiges

  Definition von Wertgrenzen (z.B. max. 35€ je Geschenk und Mitarbeiter in Zeitraum x?) --> Freigrenze Vorsteuerabzug?

  Oder 25€ (vgl. Bundesbeamten)?

  --> Lokale Gesetzgebung berücksichtigen. --> Niedrigste, global gültige Grenze ansetzen? Zeitpunkt (z.B. nicht während Vertragsverhandungen)

  Überschreitet ein Geschenk die definierte Höchstgrenze (25€ oder 35€, siehe oben), muss deren Annahme vom Vorgesetzten genehmigt werden (ggf. Prüfung durch Compliance-Verantwortlichen?).
- Geltungsbereich definieren (alle Mitarbeiter und alle Personen, die Funktionen in Namen des Unternehmens ausüben)