

# Compliance für KMU – Praxisleitfaden 2026

Arbeitsschutz • Datenschutz • Hinweisgeberschutz • Geldwäsche  
• Transparenzregister • Externe Rechtsabteilung • CMS

## 1. Arbeitsschutz

Arbeitsschutz gilt für jedes Unternehmen – unabhängig von der Mitarbeiterzahl.

- Gefährdungsbeurteilung inkl. psychischer Belastungen durchgeführt und dokumentiert
- TOP-Maßnahmen
- Jährliche Unterweisungen schriftlich dokumentiert
- Arbeitsanweisungen vorhanden
- Betriebsanweisungen für psychische Belastungen vorhanden
- Notfall- und Erste-Hilfe-Organisation festgelegt

## 2. Datenschutz (DSGVO)

Der Datenschutz betrifft jedes Unternehmen. Wesentliche Grundlagen:

- Verzeichnis der Verarbeitungstätigkeiten erstellt und aktuell gehalten
- Technische und organisatorische Maßnahmen dokumentiert
- Auftragsverarbeitungsverträge mit allen Dienstleistern abgeschlossen
- Löschkonzept und Schulungssystem vorhanden
- Datenschutzbeauftragter bestellt
- Meldung von Datenschutzvorfällen geregelt
- ggf. Datenschutz-Folgenabschätzung

## 3. Hinweisgeberschutzgesetz (HinSchG)

Ab 50 Mitarbeitenden ist eine interne Meldestelle Pflicht.

- Interne Meldestelle benannt
- Meldekanal eingerichtet
- Eingang einer Meldung innerhalb von 7 Tagen bestätigt
- Rückmeldung innerhalb von 3 Monaten vorgesehen
- Dokumentation aller Meldungen
- Schutz vor Repressalien gewährleistet
- Sicherstellung von Vertraulichkeit/anonyme Meldung sichergestellt

## 4. Geldwäschegesetz (GwG)

Das GwG betrifft bestimmte Branchen und verpflichtet zu dokumentierten Maßnahmen.

- GwG-Pflicht geprüft
- Risikoanalyse erstellt
- Interne Sicherungsmaßnahmen/Kontrollen durchgeführt
- Schulungen durchgeführt

- Kunden- und Unternehmensprüfung (wirtschaftlich Berechtigter) beachtet
- Verdachtsmeldepflicht beachtet
- ggf. Geldwäschebeauftragten bestimmt

## 5. Transparenzregister

Für bestimmte Unternehmensformen Pflicht, insbesondere bei wirtschaftlich Berechtigten.

- Eintragungen des wirtschaftlich Berechtigten im Transparenzregister geprüft
- Änderungen zeitnah gemeldet
- Vollständigkeit der Angaben sichergestellt

## 6. Externe Rechtsabteilung / Compliance-Beratung

Unterstützung durch externe Expertise für KMU.

- Externe Rechtsabteilung kontaktiert und beauftragt
- Compliance-Beratung eingeplant
- Verträge und Richtlinien geprüft
- Ansprechpartner für rechtliche Fragen benannt

## 7. Compliance Management System (CMS) implementiert

Ein pragmatisches CMS für KMU besteht aus sechs zentralen Bausteinen.

- Risikoanalyse durchgeführt
- Richtlinien & Prozesse definiert
- Mitarbeiter geschult
- Meldesystem vorhanden
- Kontrollen implementiert
- Regelmäßige Verbesserung/Evaluation geplant

## Kontakt

Für eine individuelle Compliance-Beratung oder eine externe Rechtsabteilung für Ihr KMU erreichen Sie mich jederzeit gerne:

### Ihre Ansprechpartnerin:

Rechtsanwältin **Anina Lau** – Compliance & Datenschutz

✉ E-Mail: [info@kanzlei-lau.com](mailto:info@kanzlei-lau.com)

🌐 Web: [www.kanzlei-lau.com](http://www.kanzlei-lau.com)

### Haftungsausschluss für das PDF

Diese Checkliste dient ausschließlich allgemeinen Informationszwecken und ersetzt keine individuelle Rechtsberatung. Für die Inhalte wird trotz sorgfältiger Bearbeitung keine Gewähr übernommen. Der Autor haftet nicht für Schäden, die aus der Anwendung oder Auslegung dieser Informationen entstehen.