

COMSIT – GLOBALER CODE OF CONDUCT

1. Präambel

Die ComSIT-Gruppe ist seit über 30 Jahren international im Bereich elektronischer und elektromechanischer Bauelemente tätig. Unsere Standorte in Europa, den USA und Asien/China unterliegen sehr unterschiedlichen gesetzlichen, ökologischen und sozialen Rahmenbedingungen. Wir verpflichten uns weltweit zu Integrität, Transparenz, verantwortungsvollem Handeln, Schutz von Menschenrechten, Daten und Umwelt sowie nachhaltiger Geschäftstätigkeit. Dieser globale Code of Conduct ist für alle Mitarbeitenden, Führungskräfte, Lieferanten und Geschäftspartner verbindlich.

2. Geltungsbereich

Dieser Code gilt weltweit für alle Mitarbeitenden, Standorte, Tochtergesellschaften und Geschäftsbereiche sowie alle Lieferanten, Agenten und Dienstleister. Regionale Besonderheiten werden über Addenda geregelt (USA, China). Strengere lokale Gesetze haben Vorrang.

3. Unternehmenswerte & Verhaltensgrundsätze

Unsere globalen Werte umfassen Integrität, Verantwortung, Respekt, Transparenz, Compliance und Sicherheit. Diese Werte gelten standortunabhängig.

4. Zusammenarbeit mit Kunden, Partnern und Lieferanten

Wir pflegen faire, respektvolle und professionelle Beziehungen. Wir erwarten von Partnern Rechtskonformität, Menschenrechts- und Umweltschutz, faire Arbeitsbedingungen, Transparenz und Antikorruptions-Compliance. Sorgfaltspflichten umfassen EU-Lieferkettengesetz/CSDDD, UFLPA, UK Modern Slavery Act und OECD-Richtlinien.

5. Globale Compliance, Exportkontrolle & Zoll

Wir erfüllen AWG/AWV/EU Dual-Use, EAR/ITAR/OFAC, chinesisches Exportkontrollrecht sowie UN- und WCO-Standards. Verboten sind Sanktionsumgehung, falsche Endverwendung, illegale Re-Exporte und nicht genehmigte Technologietransfers. Exportprozesse umfassen Klassifizierung, Screening, End-Use-Prüfung, Lizenzanalyse und Dokumentation.

6. Datenschutz, Informationssicherheit & Geheimhaltung

Anwendbare Gesetze: DSGVO/BDSG, CCPA/CPRA/State Acts, PIPL/DSL/CSL. Wir gewährleisten sichere Datenverarbeitung, Verschlüsselung, Need-to-Know-Zugänge und IT-Sicherheit nach ISO 27001/NIST. Vertrauliche Informationen sind zu schützen – auch nach Beschäftigungsende.

7. Anti-Korruption & Integrität

Anwendbare Standards: UN-, OECD-, UK Bribery Act, FCPA. Verboten: Bestechung, Kickbacks, verdeckte Zahlungen, Facilitation Payments, unangemessene Geschenke. Erlaubt: geringwertige, transparente Gastgeschenke.

8. Interessenkonflikte

Konflikte umfassen finanzielle Interessen, familiäre Beziehungen, Nebentätigkeiten oder private Nutzung interner Informationen. Pflicht zur Offenlegung.

9. Menschenrechte & Arbeitsbedingungen

Wir achten Menschenrechte, faire Arbeitsbedingungen, Gesundheitsschutz, Gleichbehandlung und verbieten jede Form von Belästigung, Zwangs- oder Kinderarbeit.

10. Nachhaltigkeit & Umwelt

Wir folgen ISO 14001, EU-Green-Deal-Zielen, RoHS/REACH, Emissionsreduktion, Kreislaufwirtschaft und verantwortungsvoller Entsorgung.

11. Anti-Money-Laundering (AML)

Wir verhindern Geldwäsche, Terrorismusfinanzierung und unklare Zahlungsströme. KYC, Dokumentation und transparente Zahlungswege sind verpflichtend.

12. Whistleblowing & Retaliation-Verbot

Wir bieten geschützte, anonyme Meldekanäle. Schutz gemäß EU-Whistleblower-Richtlinie, US-Dodd-Frank, chinesischen Hinweisschutzregeln. Retaliation ist verboten.

13. Governance & Verantwortlichkeit

Rollen: Global Compliance Officer, regionale Compliance Leads, Datenschutz- & Exportkontrollbeauftragte, jährliche Trainings, Audits und Managementpflichten.

14. Dokumentationspflichten

Compliance-Dokumentation erfolgt gemäß lokalen Vorschriften.

15. Schlussbestimmungen

Dieser Code wird jährlich überprüft und aktualisiert.