Compliance-Richtlinie / ABM Gruppe

Datenschutz, Informationssicherheit, Exportkontrolle und Dual-Use

Diese Richtlinie beschreibt unsere verbindlichen Mindestanforderungen für rechtmäßiges, integres und nachvollziehbares Handeln. Sie gilt für den Umgang mit personenbezogenen Daten, technischen Kundendaten, vertraulichen Informationen, digitalen Werkzeugen sowie für die Prüfung von Aufträgen mit möglichem exportkontrollrechtlichem, sanktionsrechtlichem oder sonstigem sensiblem Bezug. Einzelheiten können in ergänzenden Arbeitsanweisungen, Checklisten, Systemprozessen oder freigegebenen internen Vorgaben geregelt werden.

Inhaltsübersicht

- 1. Zielsetzung
- 2. Geltungsbereich
- 3. Grundsätze
- 4. Interne Arbeitsabläufe
- 5. Datenschutz und Vertraulichkeit
- 6. Informationssicherheit, Cloud und KI
- 7. Exportkontrolle, Sanktionen und Dual-Use
- 8. Qualität und Dokumentation
- 9. Lieferkette und Dienstleister
- 10. Kommunikation, Marketing und Recruiting
- 11. Meldung und Verbesserung

1. Zielsetzung

Ziel dieser Richtlinie ist es, normale Geschäftstätigkeit effizient zu ermöglichen und zugleich rechtliche, datenschutzbezogene, technische und exportkontrollrechtliche Risiken kontrolliert zu behandeln.

Die Prüfintensität richtet sich nach Risiko und Auftragskontext. Standardaufträge mit plausibler ziviler Nutzung werden im regulären Prozess bearbeitet. Auffällige Kunden-, Länder-, Endverwendungs-, Technik-, Zahlungs-, Liefer- oder Sanktionshinweise lösen eine vertiefte Prüfung aus.

2. Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeitenden, Führungskräfte, die Geschäftsführung der ABM Gruppe sowie externe Dienstleister und Geschäftspartner, soweit sie in Prozesse eingebunden sind oder Zugriff auf Daten erhalten.

Die ABM – Gruppe

besteht aus den Unternehmen:

- **ABM** Asset and Business Management AG - Ressourcenbeschaffung für Produktion und Vertrieb von Leiterplatten
- **PCB** Printed circuit boards GmbH - Herstellung und Vertrieb von Leiterplatten / HR
- **Precoplat** Präzisions-Leiterplatten-Technik GmbH - Vertrieb von Leiterplatten

Erfasst sind insbesondere:

- Anfrage, Angebot, Online-Kalkulation, Auftragsbearbeitung und Vertrieb,
- CAM, Arbeitsvorbereitung, Design-Rule-Check, DFM-Bewertung und technische Rückfragen,
- Fertigung, Qualitätssicherung, Versand, Reklamationsbearbeitung und Dokumentation,
- Einkauf, Lieferkette, IT, Datenschutz, Marketing, Recruiting und Personalprozesse.

3. Grundsätze

3.1 Rechtmäßigkeit und Integrität

- Geschäftsvorgänge müssen geltendem Recht, vertraglichen Pflichten, internen Vorgaben und behördlichen Anforderungen entsprechen.
- Bestechung, verdeckte Vorteile, Kick-backs, Umgehungsgeschäfte, falsche Angaben und bewusst unvollständige Dokumentation sind verboten.
- Geschäfte mit sanktionierten Personen, Organisationen oder nicht zulässigen Endverwendungen werden nicht durchgeführt.

3.2 Risikobasierung

- Prüfung, Freigabe und Dokumentation richten sich nach Sensibilität, Plausibilität und möglichen Auswirkungen des Vorgangs.
- Unklare oder auffällige Vorgänge werden vor verbindlicher Zusage, Fertigung, Lieferung oder technischer Unterstützung geklärt.
- Eine Eskalation dient der Absicherung des Vorgangs und soll normale, unauffällige Prozesse nicht unnötig blockieren.

3.3 Vertraulichkeit und Need-to-know

- Zugriff auf vertrauliche Informationen erhält nur, wer diesen Zugriff für die jeweilige Aufgabe benötigt.
- Kunden-, Projekt-, Layout-, Preis-, Vertrags-, Qualitäts- und Personaldaten werden vertraulich behandelt.
- Vertrauliche Informationen werden nicht ohne Freigabe veröffentlicht, weitergegeben oder in nicht freigegebenen digitalen Werkzeugen verarbeitet.

4. Interne Arbeitsabläufe

4.1 Technische Prüfung und Engineering-Leistungen

- Layout-, Bohr-, Fräs- und sonstige Fertigungsdaten werden im Rahmen der technischen Vorbereitung geprüft (automatisiert und/oder manuell).
- Bei Datenwidersprüchen, Herstellbarkeitsfragen, unklaren Zeichnungen oder technischen Risiken wird eine Klärung mit dem Kunden vorgenommen.
- Technische Änderungen, Zusatzleistungen oder Eingriffe in Kundendaten erfolgen nur auf Grundlage der Beauftragung, technischen Notwendigkeit oder abgestimmten Freigabe.

4.2 Online-Kalkulator und digitale Anfragekanäle

- Anfragen über Online-Kalkulator, E-Mail, Telefon oder Vertrieb werden gleichwertig in die Compliance-, Datenschutz- und Prüfprozesse einbezogen.
- Digitale Prozesse ersetzen nicht die fachliche Prüfung auffälliger oder technisch unklarer Vorgänge.
- Preis-, Lieferzeit- und Machbarkeitsaussagen erfolgen auf Grundlage der verfügbaren Daten und können bei technischen Klärungen angepasst werden, soweit dies sachlich erforderlich ist.

4.3 Rechteklärung

- Reverse Engineering und vergleichbare Leistungen werden nur umgesetzt, wenn die erforderlichen Nutzungs- und Verfügungsrechte durch den Auftraggeber geklärt sind.
- Technische Beratung dient der Herstellbarkeit und Qualität der Leiterplatten und ersetzt keine kundenseitige Produktzulassung, Sicherheitsbewertung oder Endverwendungsprüfung.

5. Datenschutz und Vertraulichkeit

Die ABM Gruppe verarbeitet personenbezogene Daten nur auf rechtmäßiger Grundlage, zweckgebunden und im erforderlichen Umfang. Dazu gehören insbesondere Kundenkontakte, Lieferantenkontakte, Bewerberdaten, Personaldaten, Kommunikationsdaten, Angebots- und Auftragsdaten.

5.1 Datenschutzgrundsätze

- **Zweckbindung:** Daten werden nur für den jeweiligen geschäftlichen oder gesetzlichen Zweck verarbeitet.
- **Datenminimierung:** Es werden nur Daten erhoben und gespeichert, die für Angebot, Vertrag, Fertigung, Lieferung, Qualitätssicherung, Dokumentation, Personalprozesse oder gesetzliche Pflichten erforderlich sind.
- **Zugriffsschutz:** Personenbezogene Daten und vertrauliche Projektdaten werden nur berechtigten Personen zugänglich gemacht.

- **Speicherbegrenzung:** Daten werden gelöscht oder archiviert, sobald sie nicht mehr erforderlich sind und keine gesetzlichen, vertraglichen oder qualitätsbezogenen Aufbewahrungsgründe bestehen.
- **Transparenz und Betroffenenrechte:** Datenschutzanfragen werden unverzüglich an die zuständige interne Stelle weitergegeben.

5.2 Technische Kundendaten

Technische Kundendaten sind besonders schutzwürdig. Dazu gehören insbesondere Gerberdaten, ODB++-Daten, Excellon-Bohrdaten, DXF-/HPGL-Zeichnungen, Eagle-/Fusion-Daten, Stücklisten, Spezifikationen, Lagenaufbauten, Prüfanforderungen, Reklamationsdaten, technische Rückfragen und sonstige projektspezifische Unterlagen.

- Technische Kundendaten werden ausschließlich für Anfrage, technische Prüfung, Angebot, Fertigung, Qualitätssicherung, Lieferung, Reklamationsbearbeitung, Dokumentation oder gesetzliche Nachweise genutzt.
- Eine Weitergabe an Dritte erfolgt nur, wenn sie zur Vertragserfüllung erforderlich, vertraglich zulässig, gesetzlich geboten oder vom Kunden freigegeben ist.
- Eine Nutzung für Werbung, Referenzen, Schulungen, Veröffentlichungen oder interne Beispielsammlungen erfolgt nur anonymisiert oder nach entsprechender Freigabe.

5.3 Bewerbungs-, Personal- und Bilddaten

- Bewerbungs- und Personaldaten werden vertraulich behandelt und nur durch die zuständigen Stellen verarbeitet.
- Entgelt-, und Personalmaßnahmen werden nachvollziehbar dokumentiert und vor Umsetzung auf arbeits-, steuer-, sozialversicherungs- und datenschutzrelevante Aspekte geprüft.
- Fotos, Videos und personenbezogene Inhalte für Marketing, Recruiting oder interne Kommunikation werden nur verwendet, wenn eine geeignete Freigabe oder sonstige zulässige Grundlage vorliegt.

6. Informationssicherheit, Cloud und KI

Die ABM Gruppe schützt Informationen durch angemessene technische und organisatorische Maßnahmen. Dazu gehören Berechtigungskonzepte, sichere Übertragung, Datensicherung, Schutz vor Malware und Phishing, geregelte Ablage, Passwortschutz und Sensibilisierung der Mitarbeitenden.

6.1 Digitale Werkzeuge

- Für vertrauliche Kunden-, Projekt-, Layout-, Preis-, Vertrags-, Qualitäts- und Personaldaten dürfen nur freigegebene Systeme und Übertragungswege genutzt werden.
- Bei der Auswahl und Freigabe externer Cloud-, KI-, Übersetzungs-, Analyse- oder Konvertierungswerkzeuge werden Anbieter, Rechenzentren und Datenverarbeitungen innerhalb der EU/EWR bevorzugt, soweit dies fachlich, technisch und wirtschaftlich angemessen möglich ist.
- Eine Verarbeitung außerhalb der EU/EWR erfolgt nur, wenn Datenschutz, Vertraulichkeit, Rechte, Speicherort, Auftragsverarbeitung, Zugriffsschutz und erforderliche Transfermechanismen geprüft und freigegeben sind.
- Besonders sensible technische Daten werden nicht in öffentliche oder private KI-Systeme eingegeben, sofern keine ausdrückliche Freigabe und geeignete Schutzmaßnahmen bestehen.

6.2 Sicherheitsvorfälle

Fehlversendungen, Verlust von Datenträgern, unberechtigter Zugriff, Phishing, Malware, Verdacht auf Datenabfluss oder irrtümliche Offenlegung sind unverzüglich intern zu melden. Die zuständige Stelle bewertet Meldepflichten, Abhilfemaßnahmen und Dokumentation.

7. Exportkontrolle, Sanktionen und Dual-Use

Leiterplatten und technische Informationen können je nach Spezifikation, Endverwendung, Empfänger, Zielland oder Projektkontext exportkontrollrechtlich relevant sein. Deshalb erfolgt eine risikobasierte Prüfung von Aufträgen, Lieferungen, technischer Unterstützung und relevanten Drittzugriffen.

7.1 Prüfanlässe

Eine vertiefte Prüfung ist insbesondere erforderlich bei:

- militärischem, sicherheitskritischem oder behördlich reguliertem Endverwendungsbezug,
- Exporten, Lieferungen oder technischer Unterstützung außerhalb der EU,
- Embargo-, Sanktions- oder Risikoländer,
- unklarem Endkunden, unklarer Endverwendung oder auffälligen Liefer-/Zahlungswegen,
- technischen Merkmalen, die eine Nähe zu Dual-Use- oder Rüstungsgüterlisten vermuten lassen,
- Widersprüchen zwischen Kunde, Besteller, Rechnungsempfänger, Lieferadresse, Endkunde oder Verwendungszweck.

7.2 Prüfung

- Kunde, Empfänger, wirtschaftlich Beteiligte, Lieferland, Zahlungsweg und Endverwendung werden risikobasiert auf Plausibilität geprüft.
- Technische Merkmale werden bei Bedarf mit den einschlägigen Güterlisten abgeglichen.
- Bei unklarer Einstufung, Genehmigungspflicht oder Endverwendung wird der Vorgang intern eskaliert und gegebenenfalls externe Fachberatung oder eine zuständige Behörde einbezogen.
- Eine Lieferung, technische Unterstützung oder Datenweitergabe erfolgt erst, wenn bestehende "Rot-Einstufungen" geklärt und erforderliche Freigaben oder Genehmigungen vorliegen.

7.3 Prüf- und Freigabeprozess

Die Freigabe sensibler Vorgänge erfolgt nach einer Ampellogik.

Status	Beschreibung	Maßnahme
Grün	Unauffälliger Vorgang mit plausibler ziviler Nutzung und ohne erkennbare Sanktions-, Embargo-, Endverwendungs- oder technische Risikohinweise. Dies gilt insbesondere für nachvollziehbare Re-Aufträge.	Bearbeitung im normalen Prozess. Eine gesonderte Einzelfallfreigabe ist nicht erforderlich, soweit im Prozess keine neuen Risikohinweise auftreten.
Gelb	Einzelne Unklarheiten oder erhöhte Sensibilität, z. B. unvollständige Endverwendungsinformationen, auffällige technische Anforderungen, besondere Dokumentationsanforderungen oder nicht vollständig plausible Beteiligte.	Klärung vor Fortführung des Vorgangs. Entscheidung und wesentliche Prüfgrundlagen werden nachvollziehbar dokumentiert.
Rot	Sanktions-, Embargo-, Genehmigungs-, Umgehungs-, Endverwendungs- oder erhebliche Plausibilitätsrisiken, insbesondere bei gelisteten Personen oder Organisationen, Embargo-/Sanktionsbezug oder nicht plausibel geklärter Endverwendung.	Der Vorgang wird nicht angenommen bzw. gestoppt. Es erfolgen keine Fertigung, Lieferung, technische Unterstützung oder Datenweitergabe. Eine Fortführung ist nur möglich, wenn der Risikohinweis vollständig ausgeräumt ist, keine Verbote entgegenstehen und erforderliche Genehmigungen sowie interne Freigaben dokumentiert vorliegen.

7.4 Dokumentation

Wesentliche Prüfungen, Rückfragen, Kundenangaben, Endverwendungsinformationen, technische Einstufungen, Freigaben, Ablehnungen und gegebenenfalls behördliche oder externe Stellungnahmen werden nachvollziehbar im Vorgang dokumentiert. Vorgänge der Ampelstufe „Grün“ bedürfen keiner zusätzlichen Einzelfalldokumentation außerhalb der regulären System- und Auftragsdokumentation.

8. Qualität, Rückverfolgbarkeit und Dokumentation

Qualität und nachvollziehbare Fertigung sind Teil der Compliance. Wir arbeiten mit definierten technischen Lieferbedingungen, Qualitätsstandards, Prüfprozessen und Dokumentationsanforderungen.

- Fertigungsdaten werden technisch geprüft und auf Herstellbarkeit vorbereitet.
- Prüfanforderungen, Sonderanforderungen und kundenspezifische Vorgaben werden durch die zuständigen Bereiche bewertet.
- Produktions-, Prüf- und qualitätsrelevante Informationen werden gemäß internen Vorgaben und relevanten Aufbewahrungsanforderungen dokumentiert.
- Reklamationen, technische Abweichungen und Korrekturmaßnahmen werden nachvollziehbar bearbeitet.

9. Lieferkette und Dienstleister

Lieferanten, Dienstleister und sonstige Geschäftspartner werden risikobasiert ausgewählt und gesteuert. Besonders relevant sind Drittzugriffe auf technische Kundendaten, IT-Systeme, personenbezogene Daten, Fertigungsleistungen oder qualitätskritische Prozesse.

- Dienstleister erhalten nur Zugriff auf Daten und Systeme, soweit dies für ihre Leistung erforderlich ist.
- Vertraulichkeit, Datenschutz, IT-Sicherheit, Qualität und Exportkontrollanforderungen werden angemessen berücksichtigt.

- Bei ausgelagerten Leistungen oder Drittzugriffen auf vertrauliche Daten werden geeignete vertragliche und organisatorische Schutzmaßnahmen vereinbart.
- Material- und Prozessentscheidungen berücksichtigen technische Anforderungen, Verfügbarkeit, Qualität und, soweit möglich, ressourcenschonende Fertigung.

10. Kommunikation, Marketing und Recruiting

Öffentliche Kommunikation ist sachlich, überprüfbar und mit der Unternehmenskommunikation abgestimmt. Aussagen zu Fertigung, Standort, Qualität, Nachhaltigkeit, Zertifizierungen, Branchen, Normen, Prüfungen, Lieferzeiten oder technischen Fähigkeiten müssen zutreffend und belegbar sein.

- Kunden-, Projekt-, Layout- und Fertigungsdaten werden nicht ohne Freigabe veröffentlicht.
- Vergleiche mit Wettbewerbern, Qualitätsversprechen und Aussagen zu „Made in Germany“ oder Nachhaltigkeit erfolgen nur, wenn sie sachlich zutreffend und belegbar sind.
- Recruiting- und Personalmarketing-Inhalte werden diskriminierungsfrei, transparent und datenschutzkonform erstellt.
- Personenbezogene Bilder, Namen oder Aussagen werden nur nach Freigabe oder auf sonstiger zulässiger Grundlage verwendet.

11. Meldung, Verantwortlichkeit und Verbesserung

Alle Mitarbeitenden sind verpflichtet, erkennbare Verstöße, Verdachtsfälle oder wesentliche Risiken unverzüglich der Geschäftsführung oder über die zuständigen internen Meldewege zu melden. Datenschutzvorfälle sind unverzüglich an die zuständige Datenschutzstelle bzw. den Datenschutzbeauftragten weiterzugeben. Die typischen Prüfbereiche und Leitfragen hierzu sind in Anlage 1 und 2 aufgeführt.

Hinweisgeberschutz (Whistleblowing): Meldende Mitarbeitende (Hinweisgebende) sind gesetzlich geschützt. Ihnen entstehen durch eine Meldung in gutem Glauben keinerlei berufliche oder persönliche Nachteile.

Die Geschäftsführung trägt die Gesamtverantwortung für Compliance. Die operative Umsetzung erfolgt in den jeweils zuständigen Bereichen durch die Abteilungsleiter. Diese Richtlinie wird regelmäßig und anlassbezogen überprüft, insbesondere bei neuen gesetzlichen Anforderungen, neuen digitalen Werkzeugen, geänderten Kundensegmenten, sicherheitskritischen Projekten oder wesentlichen Prozessänderungen.

Datum: _____

Unterschrift: _____

Anlagen

Anlage 1: Typische Prüffragen bei sensiblen Vorgängen

Prüfbereich	Leitfragen
Kunde / Beteiligte	Ist der Kunde bekannt und plausibel? Gibt es abweichende Besteller, Rechnungsempfänger, Lieferadressen oder Endkunden? Gibt es Sanktions- oder Embargohinweise?
Land / Lieferung	Liegt die Lieferung innerhalb der EU oder in ein Drittland? Gibt es Embargo-, Sanktions- oder Hochrisikobezug? Ist die Lieferroute plausibel?
Endverwendung	Ist die Endverwendung bekannt und plausibel? Gibt es Hinweise auf militärische, sicherheitskritische, nukleare, trägertechnische oder sonstige regulierte Verwendung?
Technik	Gibt es technische Merkmale, Spezifikationen, Materialien, Toleranzen, Dokumentationsanforderungen oder Normbezüge, die eine vertiefte Einstufung erforderlich machen?
Daten / Geheimhaltung	Sind besondere Vertraulichkeitsanforderungen, Schutzklassifizierungen, kundenseitige NDA-Vorgaben oder Einschränkungen für Drittzugriffe vorhanden?
Plausibilität	Passen Menge, Preis, Lieferzeit, technische Anforderungen, Geschäftszweck und Kommunikation zusammen? Gibt es ungewöhnlichen Zeitdruck oder Ausweichverhalten?

Anlage 2: Datenklassifikation

Klasse	Beispiele	Umgang
Öffentlich	Freigegebene Website-Inhalte, öffentliche Produktinformationen, freigegebene Stellenanzeigen	Kann veröffentlicht werden, sofern Urheber-, Persönlichkeits- und Datenschutzrechte beachtet werden.
Intern	Interne Prozessinformationen, interne Vorlagen, nicht veröffentlichte Planungen	Nur intern oder für berechtigte Dienstleister nutzbar.
Vertraulich	Kundenlayouts, Gerber-/ODB++-/Bohrdaten, Angebote, Preise, technische Rückfragen, Reklamationen	Need-to-know, geregelte Ablage, keine Veröffentlichung, keine nicht freigegebenen Tools.
Besonders sensibel	Sicherheitskritische Projekte, personenbezogene Daten, Personalakten, sensible Endverwendungsinformationen, NDA-geschützte Projektdaten	Erhöhte Zugriffsbeschränkung, dokumentierte Freigabe, besondere Sorgfalt bei Weitergabe und Verarbeitung.

Anlage 3: Rechtsgrundlagen und Orientierungshilfen

- European Data Protection Board: Grundlegende Verarbeitungsgrundsätze der DSGVO
- European Data Protection Board: Datenschutz durch Design und Nachweisbarkeit der Einhaltung
- Verordnung (EU) 2021/821 - EU-Dual-Use-Verordnung
- BAFA: Güterlisten, EU-Dual-Use-Verordnung und Ausfuhrliste
- BAFA: Ausfuhrverantwortlicher und ICP-Hinweise
- Datenschutzerklärung - Precoplat
- Technische Lieferbedingungen (TLB) - Precoplat
- Download Center - Dokumente für Sie zusammengestellt - Precoplat