

Version	Document	
1.1 23 June 2026 16:01	Compliance Guidelines	

Compliance Guidelines / ABM Group

Data Protection, Information Security, Export Control and Dual-Use

This policy sets out our binding minimum requirements for lawful, ethical and transparent conduct. It applies to the handling of personal data, technical customer data, confidential information and digital tools, as well as to the review of orders with potential implications under export control legislation, sanctions legislation or other sensitive matters. Further details may be set out in supplementary work instructions, checklists, system processes or approved internal guidelines.

Table of Contents

- [1. Objective](#)
- [2. Scope](#)
- [3. Principles](#)
- [4. Internal Workflows](#)
- [5. Data protection and confidentiality](#)
- [6. Information security, cloud computing and AI](#)
- [7. Export controls, sanctions and dual-use](#)
- [8. Quality and Documentation](#)
- [9. Supply chain and service providers](#)
- [10. Communication, marketing and recruitment](#)
- [11. Reporting and Improvement](#)

1. Objective

The aim of this policy is to facilitate normal business operations efficiently whilst managing legal, data protection, technical and export control risks in a controlled manner.

The level of scrutiny depends on the risk and the context of the order. Standard orders with a plausible civilian use are processed through the regular procedure. Any unusual information regarding customers, countries, end-use, technology, payment, delivery or sanctions triggers an in-depth review.

2. Scope

This policy applies to all employees, managers, the executive board of the ABM Group, as well as external service providers and business partners, insofar as they are involved in processes or have access to data.

The ABM Group

consists of the following companies:

- **ABM** Asset and Business Management AG – procurement of resources for the production and distribution of printed circuit boards
- **PCB** Printed circuit boards GmbH – manufacture and distribution of printed circuit boards / HR
- **Precoplat** Präzisions-Leiterplatten-Technik GmbH – distribution of printed circuit boards

In particular, the following are covered:

- Enquiries, quotations, online costing, order processing and sales,
- CAM, work planning, design rule checking, DFM assessment and technical enquiries,
- Manufacturing, quality assurance, dispatch, complaints handling and documentation,
- Purchasing, supply chain, IT, data protection, marketing, recruitment and HR processes.

3. Principles

3.1 Legality and Integrity

- Business transactions must comply with applicable law, contractual obligations, internal guidelines and regulatory requirements.
- Bribery, hidden benefits, kickbacks, circumvention schemes, false statements and deliberately incomplete documentation are prohibited.
- No business is conducted with sanctioned individuals, organisations or for unauthorised end uses.

3.2 Risk-based approach

- Review, approval and documentation are determined by the sensitivity, plausibility and potential impact of the transaction.
- Unclear or suspicious transactions are clarified before a binding commitment is made, production commences, delivery takes place or technical support is provided.
- Escalation serves to safeguard the transaction and should not unnecessarily block normal, unremarkable processes.

3.3 Confidentiality and need-to-know

- Access to confidential information is granted only to those who require it for the task at hand.
- Customer, project, layout, pricing, contractual, quality and personnel data are treated as confidential.
- Confidential information is not published, disclosed or processed in unauthorised digital tools without authorisation.

4. Internal Workflows

4.1 Technical Review and Engineering Services

- Layout, drilling, milling and other manufacturing data are checked as part of the technical preparation process (automatically and/or manually).
- In the event of data discrepancies, manufacturability issues, unclear drawings or technical risks, clarification is sought from the customer.
- Technical changes, additional services or modifications to customer data are carried out only on the basis of the order, technical necessity or agreed approval.

4.2 Online Calculator and Digital Enquiry Channels

- Enquiries via the online calculator, email, telephone or the sales department are treated equally within the compliance, data protection and verification processes.
- Digital processes do not replace the technical review of conspicuous or technically unclear processes.
- Statements regarding price, delivery time and feasibility are made on the basis of the available data and may be adjusted following technical clarification, insofar as this is objectively necessary.

4.3 Clarification of rights

- Reverse engineering and similar services are only carried out if the necessary rights of use and disposal have been clarified by the client.
- Technical consultancy is intended to ensure the manufacturability and quality of the printed circuit boards and does not replace any product approval, safety assessment or end-use verification required by the client.

5. Data Protection and Confidentiality

The ABM Group processes personal data only on a lawful basis, for specific purposes and to the extent necessary. This includes, in particular, customer contacts, supplier contacts, applicant data, personnel data, communication data, and quotation and order data.

5.1 Data protection principles

- **Purpose limitation:** Data is processed only for the relevant business or legal purpose.
- **Data minimisation:** Only data necessary for quotations, contracts, manufacturing, delivery, quality assurance, documentation, HR processes or legal obligations is collected and stored.
- **Access control:** Personal data and confidential project data are made accessible only to authorised persons.

- **Storage limitation:** Data is deleted or archived as soon as it is no longer required and there are no legal, contractual or quality-related grounds for retention.
- **Transparency and data subjects' rights:** Data protection enquiries are forwarded immediately to the relevant internal department.

5.2 Technical customer data

Technical customer data is particularly sensitive. This includes, in particular, Gerber data, ODB++ data, Excellon drilling data, DXF/HPGL drawings, Eagle/Fusion data, bills of materials, specifications, layer structures, testing requirements, complaints data, technical enquiries and other project-specific documents.

- Technical customer data is used exclusively for enquiries, technical reviews, quotations, manufacturing, quality assurance, delivery, complaint handling, documentation or statutory records.
- Data will only be disclosed to third parties if this is necessary for the fulfilment of the contract, contractually permitted, required by law or authorised by the customer.
- Use for advertising, references, training, publications or internal case studies shall only take place in anonymised form or following appropriate authorisation.

5.3 Application, personnel and image data

- Job application and personnel data are treated confidentially and processed only by the relevant departments.
- Remuneration and HR measures are documented in a traceable manner and reviewed for labour, tax, social security and data protection aspects prior to implementation.
- Photographs, videos and personal content for marketing, recruitment or internal communication are only used if appropriate authorisation or another permissible basis exists.

6. Information security, cloud and AI

The ABM Group protects information through appropriate technical and organisational measures. These include access control policies, secure transmission, data backup, protection against malware and phishing, regulated storage, password protection and staff awareness training.

6.1 Digital tools

- Only approved systems and transmission channels may be used for confidential customer, project, layout, pricing, contractual, quality and personnel data.
- When selecting and approving external cloud, AI, translation, analysis or conversion tools, preference is given to providers, data centres and data processing operations within the EU/EEA, insofar as this is reasonably feasible from a professional, technical and economic perspective.
- Processing outside the EU/EEA shall only take place if data protection, confidentiality, rights, storage location, data processing on behalf of a controller, access protection and the necessary transfer mechanisms have been reviewed and approved.
- Particularly sensitive technical data shall not be entered into public or private AI systems unless explicit authorisation and appropriate safeguards are in place.

6.2 Security Incidents

Incidents such as misdirected mail, loss of data storage media, unauthorised access, phishing, malware, suspected data breaches or inadvertent disclosure must be reported internally without delay. The responsible department will assess reporting obligations, remedial measures and documentation.

7. Export controls, sanctions and dual-use

Printed circuit boards and technical information may be subject to export control regulations depending on their specification, end use, recipient, destination country or project context. Consequently, a risk-based assessment is carried out for orders, deliveries, technical support and relevant third-party access.

7.1 Triggers for review

An in-depth review is required in particular in the case of:

- end-uses relating to military, security-critical or government-regulated applications,
- exports, deliveries or technical assistance outside the EU,
- countries subject to embargoes, sanctions or deemed high-risk,
- an unclear end customer, an unclear end-use or conspicuous delivery/payment routes,
- technical characteristics suggesting a connection to dual-use or military goods lists,
- discrepancies between the customer, the person placing the order, the invoice recipient, the delivery address, the end customer or the intended use.

7.2 Verification

- The customer, recipient, economically involved party, country of delivery, payment method and end-use are checked for plausibility on a risk-based basis.
- Technical characteristics are cross-referenced with the relevant goods lists where necessary.
- In the event of unclear classification, licensing requirements or end-use, the matter is escalated internally and, where necessary, external specialist advice or a competent authority is consulted.
- A delivery, technical support or data transfer will only take place once any existing 'red classifications' have been clarified and the necessary approvals or authorisations have been obtained.

7.3 Review and Approval Process

The approval of sensitive processes follows a traffic-light system.

Status	Description	Action
Green	Unremarkable transaction with a plausible civilian use and no identifiable indications of sanctions, embargoes, end-use restrictions or technical risks. This applies in particular to verifiable repeat orders.	Processed via the standard procedure. No separate case-by-case approval is required, provided no new risk indicators arise during the process.
Yellow	Isolated ambiguities or heightened sensitivity, e.g. incomplete end-use information, conspicuous technical requirements, special documentation requirements or parties involved that are not entirely plausible.	Clarification required before proceeding. The decision and key audit evidence must be documented in a traceable manner.
Red	Risks relating to sanctions, embargoes, licences, circumvention, end-use or significant plausibility issues, particularly in the case of listed persons or organisations, links to embargoes or sanctions, or end-use that has not been plausibly clarified.	The transaction is not accepted or is halted. No manufacturing, delivery, technical support or data transfer takes place. Continuation is only possible if the risk indication has been fully resolved, no prohibitions apply and the necessary licences and internal approvals are documented and in place.

7.4 Documentation

Key checks, enquiries, customer details, end-use information, technical classifications, approvals, rejections and, where applicable, regulatory or external comments shall be documented in the case in a traceable manner. Cases classified as 'Green' require no additional case-by-case documentation beyond the regular system and order documentation.

8. Quality, Traceability and Documentation

Quality and traceable manufacturing are integral to compliance. We work in accordance with defined Technical Delivery Conditions, quality standards, inspection processes and documentation requirements.

- Production data is technically reviewed and prepared for manufacturability.
- Test requirements, special requirements and customer-specific specifications are assessed by the relevant departments.
- Information relevant to production, testing and quality is documented in accordance with internal guidelines and relevant retention requirements.
- Complaints, technical deviations and corrective actions are handled in a traceable manner.

9. Supply Chain and Service Providers

Suppliers, service providers and other business partners are selected and managed on a risk-based basis. Of particular relevance is third-party access to technical customer data, IT systems, personal data, manufacturing services or quality-critical processes.

- Service providers are only granted access to data and systems to the extent necessary for them to perform their services.
- Confidentiality, data protection, IT security, quality and export control requirements are taken into account appropriately.

Version	Document	
1.1 23 June 2026 16:01	Compliance Guidelines	

- In the case of outsourced services or third-party access to confidential data, suitable contractual and organisational safeguards are agreed.
- Decisions regarding materials and processes take into account technical requirements, availability, quality and, where possible, resource-efficient manufacturing.

10. Communication, Marketing and Recruitment

Public communications are factual, verifiable and coordinated with corporate communications. Statements regarding production, location, quality, sustainability, certifications, industries, standards, testing, lead times or technical capabilities must be accurate and verifiable.

- Customer, project, layout and production data are not published without authorisation.
- Comparisons with competitors, quality promises and statements regarding 'Made in Germany' or sustainability are only made if they are factually accurate and verifiable.
- Recruitment and HR marketing content is produced in a non-discriminatory, transparent manner and in compliance with data protection regulations.
- Images, names or statements relating to individuals shall only be used following authorisation or on some other permissible basis.

11. Reporting, Responsibility and Improvement

All employees are obliged to report any apparent breaches, suspected cases or significant risks immediately to senior management or via the relevant internal reporting channels. Data protection incidents must be reported immediately to the relevant data protection office or the Data Protection Officer. The typical areas of review and key questions in this regard are set out in Appendices 1 and 2.

Whistleblower protection: Employees who report concerns (whistleblowers) are protected by law. They shall not suffer any professional or personal disadvantages as a result of a report made in good faith.

The management bears overall responsibility for compliance. Operational implementation is carried out in the relevant departments by the heads of department. This policy is reviewed regularly and as and when necessary, in particular in the event of new legal requirements, new digital tools, changes to customer segments, security-critical projects or significant process changes.

Appendices

Appendix 1: Typical audit questions for sensitive processes

Audit area	Key questions
Customer / Parties involved	Is the customer known and plausible? Are there discrepancies regarding the purchaser, invoice recipient, delivery addresses or end customers? Are there any indications of sanctions or embargoes?
Country / Delivery	Is the delivery within the EU or to a third country? Are there any embargoes, sanctions or high-risk transactions involved? Is the delivery route plausible?
End use	Is the end use known and plausible? Are there any indications of military, security-critical, nuclear, missile-related or other regulated uses?
Technical aspects	Are there any technical characteristics, specifications, materials, tolerances, documentation requirements or references to standards that necessitate a more detailed classification?
Data / Confidentiality	Are there any specific confidentiality requirements, security classifications, customer-imposed NDA provisions or restrictions on third-party access?
Plausibility	Do the quantity, price, delivery time, technical requirements, business purpose and communication all align? Is there any unusual time pressure or evasive behaviour?

Appendix 2: Data Classification

Class	Examples	Handling
Public	Approved website content, public product information, approved job advertisements	May be published provided that copyright, personal rights and data protection rights are observed.
Internal	Internal process information, internal templates, unpublished plans	May only be used internally or by authorised service providers.
Confidential	Customer layouts, Gerber/ODB++/drilling data, quotations, prices, technical enquiries, complaints	Need-to-know basis, regulated storage, no publication, no unauthorised tools.
Highly sensitive	Security-critical projects, personal data, personnel files, sensitive end-use information, NDA-protected project data	Enhanced access restrictions, documented authorisation, particular care taken when sharing and processing.

Appendix 3: Legal bases and guidance

- [European Data Protection Board: Fundamental processing principles of the GDPR](#)
- [European Data Protection Board: Data Protection by Design and Demonstrable Compliance](#)
- [Regulation \(EU\) 2021/821 – EU Dual-Use Regulation](#)
- [BAFA: Lists of goods, EU Dual-Use Regulation and Export List](#)
- [BAFA: Export control officer and ICP guidance](#)
- [Privacy Policy – Precoplat](#)
- [Technical Delivery Conditions \(TLB\) – Precoplat](#)
- [Download Centre – Documents compiled for you – Precoplat](#)