

Confidentiality: Confidentiality as the Foundation of Industrial Procurement

Confidentiality refers to the obligation to protect confidential information such as drawings, calculations or trade secrets from unauthorised access. In industrial procurement, it is a fundamental prerequisite for collaboration with suppliers, for example in tenders, prototype construction and long-term framework agreements. Anyone who systematically regulates confidentiality reduces the risk of knowledge outflow, imitation and negotiation disadvantages. At the same time, it fulfils statutory duties to protect trade secrets.

Key facts

- Confidentiality protects company information such as drawings, bills of materials, calculations and prices from unauthorised disclosure.
- The legal basis is usually confidentiality agreements (NDAs) supplemented by clauses in terms and conditions of purchase and framework agreements.
- In Germany, protection is based primarily on the German Trade Secrets Act (GeschGehG), supplemented by data protection law for personal data.
- Confidentiality must be organised on a role basis: need-to-know principle, defined contacts and documented releases.
- Typical weak points lie with sub-suppliers, external service providers and uncontrolled data exchange via email or private channels.
- Compliance is part of contract compliance and should be audited regularly.

Definition: confidentiality

Confidentiality is the duty to use information classified as confidential only for the agreed purpose and not to make it accessible to third parties. It encompasses both contractual obligations and organisational and technical protective measures.

Distinction from other protective rights

Confidentiality is not the same as industrial property rights: patents and trademarks protect inventions and marks through state registration, while confidentiality is agreed contractually. Know-how can also be protected through secrecy without registration, provided the requirements under the GeschGehG are met – such as appropriate confidentiality measures. In practice, companies combine both approaches depending on protection needs.

- Patents: registered, time-limited protection of technical inventions
- Trade secret: protection only with demonstrable, appropriate confidentiality measures
- Copyright: protection of software and documentation without registration

Confidential information in procurement

The focus is on technical drawings, specifications, bills of materials, cost breakdown and open-book calculation, price and volume data from volume tiers and blanket orders, as well as supplier evaluations. Strategic documents such as the procurement business plan or tender documents prior to a tender are also confidential. Anyone who delimits and classifies this data can implement protective measures in a targeted and proportionate manner.

Contractual foundations and regulatory instruments

Contractual protection begins before the first data exchange and runs through the entire supplier relationship. The key instruments are NDAs, clauses in terms and conditions of purchase and specific supplementary agreements.

Confidentiality agreement (NDA)

An NDA (non-disclosure agreement) governs, before the contract is concluded, which information is protected, how long the obligation applies and what exceptions exist. In practice, the term of the confidentiality obligation after the end of the contract is typically three to five years, often longer for core know-how. Clear definitions, contractual penalties or liquidated damages, and the right to return or destroy documents are important.

Terms and conditions of purchase and framework agreements

In terms and conditions of purchase, a confidentiality clause should continue the NDA obligation, define the circle of authorised recipients and regulate disclosure obligations towards authorities. Framework agreements supplement this with consultation rights for changes and notification obligations in the event of incidents. This keeps protection in place throughout the entire life cycle of the supplier relationship.

Disclosure to sub-suppliers

A common practical issue is the onward disclosure of confidential documents to sub-suppliers, for example in material substitution (ESG) or with relocated production processes. The prime supplier should only be permitted to disclose with prior consent and pass on the obligations unchanged and to the same depth. Back-to-back agreements with sub-tier suppliers must be verifiable through documentation.

Organisational and technical measures

Contractual obligations only take effect if they are lived organisationally. Need-to-know, data room concepts and sound supplier management underpin the practical implementation.

Need-to-know and information classification

Confidential information is classified in tiers – for example public, internal, confidential, strictly confidential. Only persons with an actual need receive access; access is logged and periodically reviewed. In the supplier audit and within the framework of KYC in procurement, compliance with internal confidentiality standards can be included as a review point.

Secure data exchange

Email attachments and unencrypted cloud storage are considered risk channels in practice. Proven solutions are protected data rooms with access rights, watermarks, download logs and automatic expiry of permissions – for example in a tender. In a data room or supplier portal, a structured spend taxonomy

and material group hierarchy help restrict access granularly to relevant material groups.

Contract end and data clean-up

After the end of the contract, documents must be returned or destroyed – physically and digitally. Documented data clean-up when changing suppliers or at project completion includes backup copies, local copies and ERP access. Remaining terms of confidentiality obligations are monitored in a contract table.

Risks, breaches and controls

Breaches of confidentiality can be economically significant – from direct competition to price disadvantages to liability towards customers. Controls and clear sanctions minimise the risk.

Typical risk situations

Risks arise particularly when changing suppliers, in the event of a change of control at the supplier, insolvency or when employees move internally to a supplier. The use of external service providers for development or cost breakdown also carries outflow risks. A bow-tie analysis can help systematically link causes with preventive and response measures.

Contractual sanctions and rights

Proven measures include contractual penalties for proven breaches, a right to temporarily suspend supply, and termination for cause in the event of serious or repeated violations. In addition, cease-and-desist and removal claims as well as the right to information about recipients can be agreed. Legal assessment of individual cases remains reserved for expert review.

Preventive control and monitoring

Regular spot checks in supplier audits, log evaluations from data rooms and contract compliance reviews are part of process optimisation in procurement. Anyone who embeds confidentiality clauses in an existing compliance and audit programme detects deviations early. Documented measures also demonstrate appropriateness within the meaning of the GeschGehG.

Confidentiality in tenders and negotiations

Especially in the early phases of collaboration – enquiry, negotiation, prototype phase – the risk of outflow is high because information must be shared without an order being in place.

Tenders with controlled information disclosure

In the bidding phase, suppliers should initially only receive the information necessary for a robust offer – for example functional requirements instead of complete drawings. An NDA before the release of detailed documents and clear rules for return after the end of the tender are standard. This preserves one's own negotiating position.

Price and cost transparency

The disclosure of cost breakdown or open-book calculation requires special protection, as it reveals price negotiations and competitive positions. A most-favoured-customer clause with the supplier may contain business-critical price information in this context. In addition, purpose limitation and non-disclosure obligations for cost data should be expressly agreed.

Current developments: digitalisation and compliance

Digital data exchange, supply chain compliance and growing awareness of know-how protection are changing the implementation of confidentiality in procurement.

Platforms, portals and supplier integration

Supplier enablement and digital supplier portals standardise data exchange but do not replace the contractual basis: access rights, logging and confidentiality obligations must be coordinated. Operationally sensitive data can also arise in electronic commercial invoice processes or in the exchange of delivery dates within the S&OP cycle. Confidentiality requirements must therefore be planned into the system architecture and interfaces.

Supply chain, sustainability and data sharing

Sustainability requirements and the EU taxonomy require the exchange of supplier data along the entire chain – for example on CO2 values or proof of origin. In practice, the tension between transparency obligations and confidentiality is often resolved through aggregated, anonymised data solutions. Clear agreements on which data may be shared are central here.

Employee and culture issues

Confidentiality fails less often due to missing contracts than due to a lack of awareness. Training for procurement and engineering, clear escalation paths in cases of suspicion and credible role modelling by management increase the effectiveness of all technical measures. Onboarding and offboarding processes with return and deletion obligations complete the picture.

Typical metrics

NDA coverage before data exchange: 100%

Proportion of suppliers with a signed NDA before the first handover of confidential documents

Proportion of audits with confidentiality review: > 80%

Typical benchmark for critical suppliers; review point in the supplier audit

Documented data clean-up after project completion: > 95%

Proportion of completed projects with confirmation of destruction or return

Practical example

A mid-sized mechanical engineering company is developing a new special-purpose machinery concept and invites five suppliers to submit bids. Before the full drawings are released, each bidder signs an NDA with a three-year term and a contractual penalty clause; each only receives access to the documents via a protected data room with an expiry date. After the award, the successful supplier is contractually obliged to pass on machining details only to named sub-suppliers. At project completion, the manufacturer confirms the complete return and deletion of all confidential documents by means of documentation.

- NDA with term, contractual penalty and return obligation before the first detailed release
- Protected data room instead of email attachments, with access logging and automatic expiry
- Prohibition on passing on to sub-suppliers without prior written consent
- Documented data clean-up and confirmation of destruction after project completion

Conclusion

Confidentiality in industrial procurement is not a formal act but an economic protection mechanism for know-how, price position and competitive advantage. It begins with a sound NDA before the first data exchange and ends with documented data clean-up after the end of the contract. Organisational measures such as need-to-know and secure data rooms are at least as important as the contractual side. Suppliers, sub-tier suppliers and digital channels must be included, as this is where the biggest gaps arise. Anyone who systematically integrates confidentiality into terms and conditions of purchase, audits and processes demonstrably reduces risks and creates the basis for trusting, long-term supplier partnerships.

Frequently asked questions

What does confidentiality mean in procurement?

Confidentiality refers to the obligation to protect confidential information such as drawings, calculations or price data from unauthorised access. It is contractually agreed through NDAs and clauses in terms and conditions of purchase and implemented organisationally through need-to-know principles and secure data rooms. The aim is to protect trade secrets and competitive advantages.

When should an NDA be concluded in the procurement process?

Ideally before the first exchange of confidential documents, i.e. before detailed tender documents or drawings. In practice, the term of the confidentiality obligation after the end of the contract is typically three to five years, often longer for core know-how. Clear definitions, exceptions, return obligations and sanctions in the event of a breach are important.

How long does a confidentiality obligation typically apply?

Typical terms after the end of the contract are three to five years, depending on the industry and sensitivity. For core know-how or long product life cycles, significantly longer periods are also agreed. The appropriate duration should be based on the protection requirements of the information and be legally reviewed on a case-by-case basis.

What counts as confidential information in procurement?

These include drawings, bills of materials, specifications, cost breakdown, open-book calculation, price and volume data, supplier evaluations and strategic documents such as the procurement business plan. Commitments regarding order volumes under a blanket order or terms of a Service Level Agreement (SLA) are also confidential. A clear classification within the company is essential.

May a supplier pass on information to sub-suppliers?

Only if this is expressly permitted contractually or the buyer agrees in advance. In practice, it is agreed that the prime supplier passes on the confidentiality obligations unchanged and to the same depth to sub-tier suppliers and documents compliance. Without such provisions, this creates a considerable control problem for the procuring company.

What happens in the event of a breach of confidentiality?

Contractually, contractual penalties, cease-and-desist and removal claims, rights to information and extraordinary termination (termination for cause) may be considered. In addition, statutory claims under the German Trade Secrets Act (GeschGehG) may apply. As a rule, the prerequisite is that the injured party can demonstrate appropriate confidentiality measures – which is why documentation and controls

are central.