

Confidentiality level: systematically define protection levels for sensitive procurement data

The confidentiality level assigns information, documents and business data in procurement to a defined protection category. It specifies who may view, share or store which data – for example in tenders, drawings or costing documents. For buyers and suppliers, it forms the basis for non-disclosure agreements, secure data rooms and audit-proof processes across the entire supply chain.

Key facts

- The confidentiality level classifies data according to protection requirements, typically using levels such as public, internal, confidential and strictly confidential.
- It governs access rights, disclosure obligations and the obligation to return or delete data after the end of the contract.
- In the supplier selection process, it determines which documents suppliers receive in tenders and negotiations.
- It is typically underpinned by non-disclosure agreements (NDAs) and internal information security policies.
- Missing or unclear levels lead in practice to data leaks, contractual penalties and reputational damage.
- Classification should be risk-based and reviewed regularly, particularly for project tenders and design-to-value workshops.

Definition: confidentiality level

The confidentiality level is a classification level that defines the protection requirement of information within the procurement process. It specifies which individuals, roles and organisations may access an information item and which obligations apply when handling it.

Distinction from the non-disclosure agreement

The confidentiality level is an internal classification tool, whereas the non-disclosure agreement (NDA) is a legal contract between two parties. The two interact: the level describes the protection requirement of an information item, while the NDA legally obliges the recipient to handle it in a protected manner. In practice, the content of an NDA is often aligned with the levels defined within the company, for example regarding encryption obligations, restriction to named individuals or deletion after project completion. Conversely, a high confidentiality level without a signed NDA offers hardly any legal protection and should be avoided.

Typical level models in procurement

Many industrial companies work with three to four levels. Common ones are: 'public' (freely shareable, e.g. catalogue data), 'internal' (employees only), 'confidential' (sharing only by agreement, e.g. bills of materials, price calculations) and 'strictly confidential' (named individuals only, e.g. patents, prototypes, customer data). The exact design varies by industry; in the automotive and mechanical engineering environment, customer requirements often need to be taken into account as well. What is decisive is that each level has clearly defined consequences for storage, transmission and destruction.

Methods and approach: classifying data in procurement

Classification should ideally follow a uniform process: assess the protection requirement, assign the level, derive protective measures and maintain them throughout the entire source-to-contract (S2C) process. This ensures protection even across interfaces to suppliers.

Assess protection requirements and assign the level

At the start of the process, the buyer, together with the functional department and, if applicable, the legal team, assesses what damage would result from unauthorised disclosure: competitive disadvantages from price disclosure, loss of know-how from drawings, or breaches of customer obligations. The level follows from this. Documents such as requirement specifications, bills of materials, 3D data or target prices receive their level upon creation, not only at the tender stage. A mandatory indication in the document header and in requests has proven effective, so that recipients can immediately recognise the confidentiality level.

Embedding levels in the tendering process

In tenders and award procedures, the level determines which platform and which procedure apply: public catalogue data is suitable for catalogue buying, whereas confidential calculations are handled via protected data rooms with access logging. Before the award decision, only invited bidders receive sensitive documents, often only after a signed NDA. Conversely, bidders' alternative offers and ancillary quotations are also considered confidential and must not be passed on to competitors – an aspect that should be explicitly regulated in award policies.

Communicating obligations to suppliers

The level only has an effect if suppliers know and acknowledge it. Proven measures include references in request documents, binding clauses in framework agreements and brief onboarding notes for new suppliers. For long-term contracts with notice periods, the confidentiality obligation should also be agreed beyond the end of the contract, typically for periods of two to five years depending on the industry. After the end of the contract, return or deletion must be documented and evidenced.

Key KPIs for managing confidentiality

Confidentiality can be managed in a measurable way by systematically recording the degree of classification, compliance with agreements and incidents. The KPIs provide management information for internal audits and supplier evaluations.

Classification rate and NDA coverage

Two basic KPIs: the proportion of fully classified procurement documents and the proportion of supplier relationships with a valid non-disclosure agreement before the first disclosure of sensitive documents. In

practice, values above 95 per cent are considered a good benchmark; below that, protection quickly declines. Both KPIs can be derived from the e-procurement system or contract system and reviewed in regular audits.

Incidents and response times

The number of reported confidentiality breaches should be recorded, along with the time to reporting and countermeasure. A low number is not automatically positive – it may also indicate a lack of transparency. In addition, the proportion of suppliers whose access rights were revoked promptly after the end of the contract is a useful metric. In supplier evaluations, confidentiality performance can be included as a criterion alongside delivery capability and service level targets.

Risks and controls in handling confidentiality levels

The main causes of data leakage are unclear responsibilities, convenient communication over insecure channels and a lack of evidence. Targeted controls significantly reduce these risks without slowing down day-to-day procurement.

Typical risk areas

Critical issues include: sending drawings via unencrypted email, sharing price calculations with project participants without an NDA, excessively long retention periods after project completion, and unclear responsibilities when staff change. Confidentiality breaches become particularly serious when they affect customer contracts or regulatory obligations – for example on orders where the customer owns tools and documents. Here, the risks include not only contractual penalties but also the loss of supply orders. Monetarily relevant documents such as bonus agreements, price index linkages or payment terms are also often subject to high levels when it comes to third parties.

Control instruments and organisation

Effective controls include: role-based access concepts in e-procurement and PLM, logged data rooms for tenders, the four-eyes principle for approving strictly confidential data, and regular spot checks to verify that documents with a level actually reside only in approved systems. A clear escalation rule is important: anyone who identifies a suspected breach reports it immediately to procurement, the data protection officer and, if applicable, the legal department. Legal consequences – such as claims under the NDA or competition law issues – should always be assessed on a case-by-case basis; this article does not constitute legal advice.

Confidentiality and international procurement

In global supply chains, language barriers, differing legal systems and country-specific expectations regarding data disclosure come into play. Contracts should therefore regulate the applicable legal system and the handling instructions for the confidentiality level in multiple languages and unambiguously. The same applies to international delivery terms such as Incoterms DAP or Incoterms CFR: documents relating to customs, freight costs and currency risk in procurement can themselves be sensitive, for example when they provide insight into margin structures or supplier terms. The level should therefore be applied to the entire document set of the procurement process, not only to technical drawings.

Current developments: digitalisation and cybersecurity

Digitalisation is fundamentally changing how confidentiality levels are handled: cloud platforms, automated requests and growing cyber threats require technical implementation of the levels rather than purely paper-based rules.

Automated classification and data rooms

Modern procurement and document management systems can classify documents automatically based on metadata, templates or content signals and derive access rights accordingly. Data rooms with two-factor authentication, watermarking and download logging are becoming the standard for tenders with a high level. This makes it possible to trace who accessed which drawing or calculation and when – a significant improvement over email distribution lists. The prerequisite is that the level logic is properly mapped in the system and cannot be circumvented by individual users.

Cybersecurity requirements for suppliers

More and more customers are demanding verifiable information security standards from suppliers, for example certifications or self-assessments on IT security. This makes confidentiality part of supplier qualification – analogous to quality and sustainability requirements such as Science Based Targets in the supply chain. Buyers should align security requirements in tiers with the confidentiality level: anyone processing strictly confidential design data needs stricter evidence than a supplier of purely public catalogue items. This keeps the effort proportionate for small suppliers.

Confidentiality level in adjacent procurement processes

The confidentiality level is not an isolated topic: it touches on the requisition, contract, goods flow and payment. Anyone who applies it consistently across all process steps avoids protection gaps and duplicate work.

From requisition to contract

In the requisition process, the level defines which suppliers may see which documents before the requisition-to-purchase-order cycle time begins and the requirement is converted into a purchase order. In negotiations, disclosure limits are sensible: target prices and alternative calculations remain confidential, while technical specifications can be shared earlier. In the framework agreement, the level is translated into clauses on confidentiality, use of the data exclusively for the agreed purpose and cascading to subcontractors.

Goods flow, quality and evidence

Sensitive data is also generated after the order is awarded: inspection results from incoming goods AQL sampling, process data, complaints and certificates such as the long-term supplier declaration (LLE) can be competition- or security-relevant. Safety time buffers and capacity agreements with suppliers also reveal much about a company's planning situation. A consistent level logic ensures that this data enjoys the same protection in partner communication, during audits and in supplier portals as the original tender documents.

Typical metrics

Classification rate of sensitive documents: > 95%

Proportion of procurement documents fully marked with a confidentiality level

NDA coverage before sensitive disclosure: > 98%

Proportion of suppliers with a valid non-disclosure agreement before initial transmission

Reported confidentiality incidents: trend: declining

Absolute number per year; interpret low figures only with sufficient reporting transparency

Access revocation rate after contract end: > 95%

Proportion of supplier access rights revoked promptly after contract or project end

Practical example

A medium-sized mechanical engineering company developed a new construction machinery assembly and invited several suppliers to a design-to-value workshop. Initially, all participants received unprotected drawings by email; after an internal review, the company introduced a tiered classification concept and implemented it consistently.

- Introduction of four confidentiality levels with mandatory indication in the document header and training for all buyers
- Migration of sensitive tenders to a logged data room with an NDA obligation before access is granted
- Anchoring of confidentiality, deletion and cascading rules in all framework agreements, including effect beyond the contract beyond the notice period
- Inclusion of confidentiality performance as a criterion in the annual supplier evaluation

Conclusion

The confidentiality level is a simple tool with a great impact: it creates clarity about which information must be protected and how within the procurement process. What is decisive is consistency of implementation – from document creation through the tender to deletion after the end of the contract. Those who interlink levels, systems and contracts significantly reduce the risk of know-how leakage and frictional losses. At the same time, the procurement function gains credibility with customers and partners. A risk-based, lean classification approach is better than an overly complex level model that gets bypassed in day-to-day practice.

Frequently asked questions

What does confidentiality level mean in procurement?

The confidentiality level is a classification level that defines how sensitive a piece of information is and who may view or share it. Typical levels are public, internal, confidential and strictly confidential. It governs protective measures such as NDA obligations, encrypted transmission and restricted access.

Which confidentiality levels are common?

In practice, three to four levels have become established: public, internal, confidential and strictly confidential. The exact naming varies by company and industry. What matters is that each level has clearly defined consequences for storage, transmission and destruction.

Who determines the confidentiality level of a document?

Ideally, the document's creator together with the relevant functional department; in procurement,

together with the requester. Many companies embed the classification obligation directly in templates and processes. In unclear cases, a defined escalation route applies, for example to the data protection officer or legal department.

Is a confidentiality level legally effective without an NDA?

An internal level primarily governs the conduct of one's own employees; it only takes legal effect against external providers once a signed non-disclosure agreement is in place. Confidential documents should therefore in principle only be shared after an NDA has been signed. The specific legal protection should be assessed on a case-by-case basis.

How long does confidentiality apply after the end of a contract?

The parties often agree that confidentiality continues beyond the end of the contract, typically two to five years in practice depending on sensitivity. For particularly sensitive data such as prototypes or customer secrets, longer periods may also be sensible. The duration should be explicitly stated in the contract.

How do you implement confidentiality levels technically?

Proven measures include role-based access concepts in e-procurement and document systems, logged data rooms for tenders, and automated classification via metadata. Watermarks and download logs improve traceability. It is important that workarounds such as private email accounts are prevented through policies and awareness measures.