

Technical Data & Confidentiality - DPPPrep

How we approach product files during a readiness or data-preparation engagement.

Before you send sensitive information

Start with one representative product and only the documents needed to understand the scope. If the files contain commercially sensitive technical information, an NDA can be agreed before transfer.

Working principles

Data minimisation	We ask for the information needed for the agreed scope rather than entire repositories by default.
Source traceability	Values are linked to evidence so assumptions and unsupported data are visible.
No data resale	Client product information is not treated as a marketing dataset or sold to third parties.
Confidentiality by agreement	NDA and project-specific handling requirements can be agreed before sensitive documents are exchanged.
Retention by scope	Retention and deletion expectations can be agreed for each engagement, including return or deletion of working copies where appropriate.
Third-party processing	Where material third-party processing is proposed for confidential data, the handling approach should be agreed as part of the engagement.
No certification claims	Data preparation does not convert unverified information into certified or legally validated data.

Recommended first transfer

A product list, one representative technical datasheet and a high-level document inventory are usually enough to scope an initial readiness review. Sensitive BOMs, detailed drawings or proprietary supplier files do not need to be sent before the scope and confidentiality arrangements are clear.

This one-pager describes DPPPrep working principles. Specific contractual confidentiality, security and retention terms are agreed in the engagement documents.