

Data protection position

Why the supplier is neither controller nor processor for your documents, what that means for a DPA, and the honest limits of the redaction and erasure functions.

1. Roles

The customer is the data controller — or, where the customer processes on behalf of its own client, the processor. **The supplier is neither.** The application transmits nothing and the supplier operates no infrastructure that receives customer data, so the supplier does not process personal data on the customer's behalf and is not a processor under Article 4(8) GDPR or a Data Processor under section 2(k) of the Digital Personal Data Protection Act 2023.

A data processing agreement is therefore not required for the software itself. Suppliers who claim otherwise are usually describing a hosted service.

2. Cross-border transfer

None. Processing takes place on the machine the software is installed on. There is no transfer to a third country under Chapter V GDPR, and no transfer outside India under section 16 of the DPDP Act.

3. What the application does for the customer's own obligations

It does not make the customer compliant, and it is not sold as doing so. Compliance is a property of the customer's practices. What the application provides is evidence and tooling for specific obligations:

OBLIGATION	WHAT THE APPLICATION PROVIDES
Article 30 GDPR — records of processing	A draft record built from what was actually processed, with the fields only the firm can answer left visibly outstanding
Article 5(1)(e) GDPR, DPDP s.8(7) — storage limitation	A retention clock anchored to a statutory basis the firm cites, and certified erasure with a hash of everything destroyed
Article 32 GDPR, DPDP s.8(5) — security of processing	Local-only processing, OS-keystore password storage, SHA-256 of every input and output
Article 17 GDPR — erasure	True redaction that removes text rather than covering it, verified by re-reading the output
DPDP s.8(3) — accuracy and completeness	Duplicate detection and a guard against one client's documents sitting in another's folder

4. Limits of the redaction and erasure functions

Stated here because a customer relying on them needs to know:

- **Redaction** removes the text from the document and the output is re-read to confirm the identifier is gone. Documents with no text layer are refused rather than covered with a rectangle.
- **Erasure** overwrites and unlinks, which is NIST SP 800-88 *Clear*. It is not *Purge* or *Destroy*. On a solid-state drive, wear levelling can leave the original block intact until the controller reuses it, and a copy-on-write filesystem can retain the earlier version in a snapshot. Full-disk encryption is what makes such residue worthless, and the erasure certificate records whether it was enabled.