

Privacy and redaction verification checklist

A practical pre-release review for PDFs that may contain sensitive information

Version 2026-08-16 · No signup required

Use this checklist to verify visible content, hidden document data, redaction quality, and release controls before sharing a sensitive PDF.

1. Prepare a safe review copy

- ☐ Work from a copy. Preserve the source in its original location and do not overwrite it.
- ☐ Use generated or approved test data while validating a new workflow.
- ☐ Record the intended audience, destination, and required retention policy before editing.
- ☐ Confirm whether laws, contracts, court rules, or organisational policy require specialist review.

2. Find visible sensitive content

- ☐ Search for names, email addresses, phone numbers, account references, identifiers, dates of birth, signatures, and free-text notes.
- ☐ Review every page at readable zoom, including headers, footers, stamps, marginal notes, and small print.
- ☐ Check scanned pages with OCR where appropriate, then visually confirm every OCR-derived candidate.
- ☐ Treat automated detection as a review aid, not a decision about what must be removed.

3. Inspect hidden and document-level data

- ☐ Inspect title, author, subject, keywords, creator, producer, and creation or modification dates.
- ☐ Check annotations, comments, form values, attachments, links, scripts, layers, bookmarks, named destinations, and signatures.
- ☐ Look for invisible text, text beneath images, content outside the crop box, and incremental revision history.
- ☐ Remove unsupported or unnecessary interactive features before release.

4. Apply redaction rather than visual covering

- ☐ Do not rely on a black rectangle, highlight, crop, white text, or hidden layer to remove source information.
- ☐ Redact the approved page regions so the underlying content is removed or the page is safely rasterised.
- ☐ Sanitise metadata and hidden structures separately; page redaction alone does not clear them.
- ☐ Expect digital signatures to become invalid when document content changes.

5. Validate the output

- ☐ Reopen the exported PDF in a second viewer and inspect every changed page.
- ☐ Search, select, copy, and extract text for every redacted value and unique test canary.
- ☐ Re-scan metadata, annotations, attachments, forms, scripts, layers, navigation, and revision history.
- ☐ Confirm page count, page order, orientation, readability, file size, and required accessibility features.
- ☐ If any check is inconclusive, stop release and escalate instead of describing the file as clean.

6. Record the release decision

- ☐ Record the output filename, date, reviewer, verification method, and cryptographic hash where policy permits.
- ☐ Keep a masked findings report or review note without copying sensitive source values into logs.
- ☐ Send only the minimum pages and fields the recipient actually needs.

[] Use an approved transfer channel and verify the recipient before sending.

Important limitations

- No checklist or automated scanner can guarantee detection of every sensitive value, concealment method, malformed object, or future PDF feature.
- This resource is operational guidance, not legal, compliance, accessibility, or information-security certification.
- High-risk releases should follow the organisation's approved review and escalation process.

Generated reproducibly from `src/content/resources/privacy-redaction-verification-checklist.json` by `scripts/generate-static-resources.mjs`.