

Data Handling Summary

DC Health Check · One page, plain language — incorporated into the engagement letter as a binding term.

What we collect. Operational exports only: orders and shipments, order lines, item master, locations and slotting, inventory on-hand and adjustments, receipts, and labor hours by anonymized ID and department. Consumer information is limited to ship-to ZIP codes. We never request — and ask you not to send — employee names, Social Security numbers, pay stubs, or payment card data.

If names slip through anyway. Our first processing step permanently strips employee names and any personal identifiers before analysis begins.

Where your data lives. A dedicated, access-controlled workspace for your engagement, protected by two-factor authentication, accessible to exactly one person: the principal analyst on your engagement, named in your engagement letter. Files reach us through a private upload link over encrypted (TLS) connections.

How AI is used. Analysis is assisted by commercial AI services under enterprise terms — your data is not used to train models. Wherever feasible, only aggregated and derived tables are processed rather than raw records.

Retention & deletion. Raw data files are deleted within 60 days of report delivery on your written request. Derived metrics (the computed KPIs behind your report) may be retained up to 12 months to support your Q&A window and any follow-up work, then deleted on request as well.

Benchmarks. We maintain anonymized, aggregated industry benchmarks. Nothing identifying your company, your customers, or your people is ever included.

Subprocessors. Google (storage/email), Anthropic (analysis), Stripe (payments), Dropbox (file transfer & e-signature).

If something goes wrong. We notify you within 72 hours of discovering any incident affecting your data.

Honesty note. We are a single-operator practice. We do not claim SOC 2 or ISO certification — we claim, and contractually commit to, exactly what is written here.