

Data Handling Profile

Baseline 002 | Buyer-facing information-control profile

AV project packages may contain confidential drawings, room information, network dependencies, standards, and commercial information. Cognitive AV limits access to the minimum necessary for the agreed engagement and applies the client-approved handling profile.

1. Default processing posture

External AI processing is disabled by default unless explicitly approved by the client.

Cognitive AV can perform the Pre-Award AV Plan Review without external AI processing. Human senior-engineering judgment remains responsible for material findings and the issued readiness opinion.

2. Information categories

Category	Examples	Handling intent
Project identity	Project name, sites, room counts, stakeholders, stage, and decision gate.	Use only for the agreed review and communications.
Technical records	Drawings, BOMs, specifications, room schedules, SOWs, responsibility matrices, acceptance plans, and standards.	Limit access to the review boundary; preserve revision context.
Enterprise dependencies	Network requirements, service dependencies, UC platform requirements, monitoring, and support assignments.	Review dependency identification and ownership; exclude credentials and secrets.
Commercial information	Proposals, pricing, alternates, substitutions, assumptions, and procurement timing.	Use only where necessary to evaluate scope and project risk.
Communications and findings	Clarifications, issue logs, findings, residual-risk statement, and readiness opinion.	Keep customer work product separated and access-bounded.

3. Access and separation

- Access is limited to the minimum necessary for the agreed engagement.
- Client materials and work product are kept separated from other customer engagements.
- Credentials, passwords, private keys, tokens, and other secrets should not be submitted.
- Link-based sharing with client-controlled permissions is preferred for sensitive project packages.
- Client restrictions, confidentiality terms, and approved storage locations govern the engagement where agreed.

4. Retention and deletion

Retention, return, and deletion requirements should be agreed for the engagement. Cognitive AV does not make universal zero-retention claims. Actual handling depends on the approved workflow, systems used, contractual requirements, and legal or operational obligations.

Authorized External AI Processing

5. Controls when external AI is explicitly authorized

Approved services

- Use customer-approved business/API services.
- Confirm the permitted workflow and data categories.
- Do not use consumer or personal accounts for restricted project data unless specifically approved.

Data minimization

- Submit only the information required for the approved task.
- Remove credentials, secrets, and unnecessary identifiers.
- Prefer bounded excerpts or structured extracts where sufficient.

Access and separation

- Apply least-privilege access.
- Maintain customer separation.
- Restrict outputs and source materials to authorized engagement use.

Human validation

- External AI may assist analysis or drafting only within the authorized workflow.
- Human engineering validation is required before material findings are issued.
- The readiness opinion remains a human technical advisory judgment.

6. Client-controlled decisions

Decision	Client direction
External AI use	Disabled by default; enabled only with explicit approval.
Approved services	Customer-approved business/API services or no external AI processing.
Storage location	Agreed workflow and client restrictions govern.
Retention / deletion	Defined for the engagement where required.
Sharing permissions	Client confirms that submitted links, files, and project records may be reviewed.

7. Out of scope

This profile is not a cybersecurity certification, penetration test, enterprise security assessment, legal opinion, or universal guarantee of security. Cognitive AV evaluates AV-related project dependencies and follows the agreed information-handling workflow; the client’s authorized security, legal, privacy, and procurement functions retain their respective decision authority.

8. Client preparation

- Use client-controlled secure links where possible.
- Remove credentials, secrets, personally sensitive information, and unrelated records.
- Confirm that sharing is authorized before submission.
- Identify any handling restrictions before the Document Readiness Gate is approved.