INTELLIGENT CHOICE

Data separation and access set-up

Keep website and client information apart, and give each tool only the access it needs

Version 1.1 | 28 October 2026 | Owner: Travis Shaw | Review: every 6 months | Printable blank copy

What this does. A one-off set-up, then a quarterly check: delete unused tokens and confirm each remaining token matches the table in B (see the Privacy routine). Also check whenever a workflow is added or a client engagement starts. If one token or one workflow is compromised, only the information that workflow needs is exposed. Click a box to tick it, and type in the notes boxes.

A. Keep website information apart from client information

- ☐ In Airtable, give website data (Readiness Results, Chat Requests) its own base or clearly labelled area. Do not store client work there.
- ☐ Give each client their own area (a base, or a client-named folder in the Drive). Where practical, keep the client's information in the client's own accounts.
- ☐ Do not link website tables to client tables.
- ☐ Record the layout in one line each in the Privacy register: where website data is, where each client's data is.

Notes (what you did, where it lives, anything to check)

B. One scoped token per workflow

Create a separate Airtable personal access token for each workflow. Give each one only the permissions and tables it needs, and a neutral name that reveals nothing if it leaks.

Workflow	Token name	Tables and permissions	Done
Readiness emailer	web-a	Readiness Results: read and write records	☐
Chat request handler	web-b	Chat Requests: read and write. Readiness Results: read only	☐
Summary workflow	none	No Airtable access. It stores nothing.	☐

- ☐ Swap each workflow to its own token, test it, then delete the old shared token.
- ☐ Use a neutral name in n8n (for example “Airtable web-a”), not a description of the content.

Notes (token names used, date swapped, old token deleted)

C. Keep run logs short (n8n)

- [ ] In each workflow's settings, set **Save successful executions** to off where the log is not needed. Keep failed executions. This is the main control, because pruning is fixed at 14 days.
- [ ] Pruning is set by OpenHost and is fixed at 14 days on our plan (confirmed 28 October 2026). Check the oldest run in the Executions list is no more than 14 days old.
- [ ] Record the setting and the date in the Privacy register.

Notes (settings chosen, oldest run date seen, OpenHost reply)

Done by: _____ Date: _____ Next check: _____