

AI for a DIFC wealth firm, *with the data kept at home*

AI behind the twelve jobs a wealth team does every week, with no client data touching the internet, and a file the compliance officer can sign off against the DIFC Data Protection Law and the DFSA Rulebook. Every blue word is a link to read more.

0

CLIENT RECORDS ON THE INTERNET

12

WORKFLOWS, ADVISER SIGNS EACH · DEMO

4

PHASES, FIRST PILOT IN WEEK 3

~43h

SAVED PER ADVISER / MONTH · ESTIMATE

1 · THE NEED

What the firm asked for

- No internet for client data. No client name, document or number ever sent to a cloud AI service.
- DIFC and DFSA rules met in writing. Data protection, autonomous-systems rules, outsourcing, record keeping.
- The whole process streamlined. Enquiry to annual review in one dashboard: [azizsaif.com/wealth-demo](#).

WHERE THE HOURS GO TODAY · FIVE JOBS WHERE AI WORKS

Onboarding and KYC	3 to 4 h per client, typed by hand, gaps found late	screen 3
Meeting prep and notes	30 to 45 min before, 30 after; actions slip	job 01
Portfolio checks	Quarterly spreadsheet, drift unnoticed for months	screen 5
Client updates	90 to 120 min per note, sent late	screen 9

2 · SAFEGUARDING THE DATA

Two worlds, *no link between them*

WORLD 1 · OFFLINE, IN THE OFFICE

- Encrypted file server, one folder per client
- Open-weight AI model on a machine in the same room, no internet cable ([sizing · models](#))
- Two encrypted backups, office safe + off-site, 6-year retention
- Advisers see own clients only; every open and edit logged

NO LINK

WORLD 2 · INTERNET DESK

- Prospect research, news, regulator updates
- Prompts and skills from [ai-wealth](#)
- Platform exports carried to World 1 on an approved encrypted drive
- Policy rule: no client name or number, ever

Hardware: small (Mac Studio 192 GB+ or one-GPU workstation) AED 20k to 50k, 5 to 10 staff · medium (one or two 80 GB GPUs) AED 150k+. Planning ranges, not quotes.

3 · THE RULES THIS MEETS

DIFC and DFSA, line by line

RULE	WHAT IT ASKS	WHAT THIS DOES	MORE
DIFC DP Law No. 5 of 2020	Firm is controller: lawful basis, security, client rights, breach reporting	Data never leaves the firm; access logged; retention set	DIFC
DIFC DP Regulation 10 (autonomous systems)	Name the AI system to clients, keep a human in control, keep records; high-risk uses may need an ASO	AI drafts, adviser signs; line in client agreement; audit log is the record	text · Clyde
DFSA GEN 5.3, outsourcing 5.3.21 and 5.3.22	Written supplier agreement, risk assessment, exit plan	Scope + NDA, logins returned at go-live, runbook for firm IT	GEN
DFSA record keeping	Files, reports and logs kept and retrievable, 6 years cited	Server + two offline backups, retrieval tested quarterly	GEN
DFSA AI Survey 2025	Written AI policy, accountability, AI register	Policy, register, impact assessment written in phase 1	DFSA

Summaries, not the rulebook. The compliance officer confirms each line against the current DFSA Rulebook and DIFC Commissioner guidance in phase 1.

4 · SAFEGUARDS ENFORCED BY SETTINGS

What [Claude Code](#) can lock down

ASK BEFORE ACTING

Every write, command or email needs a person's approval. Mode set by the firm.

DENY LISTS

Block `WebFetch` , `WebSearch` , `Bash(curl*)` . No way to reach out.

HOOKS THAT LOG

Every tool call writes who, what, when, which files to the audit log; a second hook blocks paths outside the client folder.

SANDBOX

Commands limited to allowed folders, so a mistake can't reach another client.

RULES IN PLAIN ENGLISH

CLAUDE .md : never recommend a product, never send without approval, always cite the page.

NO TRAINING ON YOUR DATA

Honest limit: Claude Code needs a model connection. Enterprise-cloud firms run as shown. Strict no-internet firms run an open-weight model in World 1 with the same rules; Claude Code builds and tests, never with live client data.

5 · THE FULL WORKFLOW DASHBOARD · DROP → AI DRAFTS → REVIEW QUEUE → ADVISER APPROVES → FILED AND LOGGED

#	JOB	AI DOES	HUMAN DOES	WORLD	SEE	#	JOB	AI DOES	HUMAN DOES	WORLD	SEE
1	Prospect brief	Public sources, service match, first email	Checks every fact link	2	s2	7	Equity and bond screen	House rules, reason per pass or fail	Analyst signs shortlist	1	s6
2	Onboarding pipeline	Stage per client, chases missing items	Compliance signs file	1	s3	8	Research notes	40 pages to 1, page numbers on figures	Clicks references	1	s7
3	Fact-find and KYC	Reads documents, fills fields, flags MISSING	Confirms every field	1	s4	9	News watch	Matches news to client segments	Reads primary source	2	s8
4	Meeting prep and note	Brief before, file note after	Adviser reviews	1	j1	10	Client update emails	Personal draft from own numbers	Approves, sends from mail desk	1	s9
5	Suitability report	First draft from fact-find and model	Adviser edits, signs	1	s3	11	Staff follow-ups	Actions become tasks with owner and date	Manager reviews weekly	1	s10
6	Portfolio drift	Daily check vs model, flags tolerance	Decides rebalance	1	s5	12	Audit log and verify	Logs prompt, output, approver, source	Compliance samples monthly	1	s11

1

WEEKS 1 TO 2 · FOUNDATIONS

Server, folders, roles, backups. AI-use policy, AI register, impact assessment. Compliance reviews the rules table. NDA and outsourcing agreement signed.

2

WEEKS 3 TO 4 · PILOT

Meeting prep, one adviser, beside the old way. Hours logged daily. Go or no-go on real numbers.

3

MONTH 2 · ONBOARDING

Fact-find extraction, pipeline chasers, follow-up tracker. First audit-log sample by compliance.

4

MONTHS 3 TO 4 · FULL DASHBOARD

Drift, screening, research, client emails, suitability drafts. Runbook, training, logins returned.