EnterpriseAI ◆ ae

# UAE private AI checklist

24 questions to answer before you run AI on confidential company data

## DATA

- [ ] **1. Which data will the AI read?**
  List every system and folder it will connect to: client files, contracts, email, ERP records. Anything not on the list stays disconnected.
- [ ] **2. Which of it is personal, confidential or regulated?**
  Personal data, client-privileged files, health records and financial data each carry different rules. Mark each source.
- [ ] **3. Who owns each data source?**
  Every source needs a named owner inside the company who approves what the AI may read.
- [ ] **4. What must never be used?**
  Write the exclusions down, for example HR disciplinary files or board papers, and make sure they are never indexed.

## LOCATION AND LAW

- [ ] **5. Which data law applies to us?**
  UAE mainland: Federal Decree-Law No. 45 of 2021. DIFC: DIFC Law No. 5 of 2020. ADGM: ADGM Data Protection Regulations. Health data: Federal Law No. 2 of 2019. Your legal adviser confirms which.
- [ ] **6. Where will prompts, files, answers and logs be stored?**
  Get it in writing: your own servers, a UAE data centre, or a named cloud region.
- [ ] **7. Does anything leave the UAE?**
  Check model calls, backups, monitoring tools and the provider's support access, not only the main database.
- [ ] **8. What do our client contracts allow?**
  Many client agreements restrict where client data may go. Read them before choosing where the AI runs.

## ARCHITECTURE

- [ ] **9. Is there a written solution architecture?**
  Where each service sits, how data flows in every situation, and which firewalls protect it. This comes before any server is bought.
- [ ] **10. Have the stakeholders seen it?**
  IT, legal and the business owner should agree the architecture before deployment starts, not after.
- [ ] **11. Which model, and why that one?**
  An open model hosted privately, or a commercial model in a private deployment. The reason should be the task and the data rules.
- [ ] **12. How big does the hardware really need to be?**
  A GPU is usually needed, but not the biggest one. Size it to the number of users and the workload, and test before buying more.

## ACCESS AND SECURITY

- [ ] **13. Do answers follow existing permissions?**
  A person should only get answers from documents they could already open themselves.
- [ ] **14. Is every question and answer logged?**
  Who asked what, when, and which documents the answer came from.
- [ ] **15. How is the system protected?**
  Network isolation, firewalls, encryption in storage and in transit, and a separate account for the AI.
- [ ] **16. What happens when the AI is wrong?**
  Answers show their sources, and anything high-stakes is checked by a person before it is acted on.


General guidance, not legal advice: confirm the law that applies to you with your legal adviser.

## PEOPLE AND PROCESS

- [ ] 17. Which job will it do first?
  One process, measured before and after. Not "AI for everything" on day one.
- [ ] 18. Who reviews its output?
  Name the person in the loop for each type of answer that matters.
- [ ] 19. Who is trained, and when?
  The people who will use it, before launch, on their own work.
- [ ] 20. What does success look like after eight weeks?
  Agree a measure in advance: hours saved, documents processed, questions answered.

## UPKEEP

- [ ] 21. Will it be tested on a small data set first?
  A trial run on a limited set of real data before the full launch.
- [ ] 22. Who updates the model and the software?
  A named owner and a schedule, including what happens when a newer model is released.
- [ ] 23. How are documents added and removed?
  New files indexed on a schedule; deleted files removed from the AI as well.
- [ ] 24. Can we leave?
  Code, configuration and data handed over, so another team could run it. No lock-in.

## THE ORDER OF WORK: DESIGN FIRST, HARDWARE SECOND

| | | | |
|---|---|---|---|
| 01 Draft the solution | 02 Solution architecture | 03 Stakeholder review | 04 Services |
| 05 Servers | 06 Security | 07 Small data-set test | 08 Launch |

Example from our work: a private AI deployment for a UAE real estate business, for up to 750 users and data for 5,000 clients, took 8 to 10 weeks from start to launch.

## WHICH UAE DATA LAW APPLIES?

UAE mainland: Federal Decree-Law No. 45 of 2021 (Personal Data Protection Law).
DIFC: DIFC Data Protection Law No. 5 of 2020. ADGM: ADGM Data Protection Regulations.
Health data: Federal Law No. 2 of 2019 on ICT in health fields (generally stored and processed inside the UAE).
Official overview: u.ae/en/about-the-uae/digital-uae/data/data-protection-laws

Want a second pair of eyes on your answers?
Request a consultation at enterpriseai.ae/contact · enquiries@enterpriseai.ae


General guidance, not legal advice: confirm the law that applies to you with your legal adviser.