

Where the model is allowed to see the data.

12 checks before a model sees UAE data.

NESA here means the UAE Information Assurance Regulation v1.1 (March 2020). DESC means Dubai Law No. 15 of 2024, for government entities and critical non-government entities DESC classifies. PDPL means Federal Decree-Law No. 45 of 2021. This page is not a legal opinion and not a certificate.

NESA

1. The model, the corpus, the prompts, and the logs are named assets and classified before anyone calls an API.
2. A risk treatment exists for the AI path: what may leave, what stays, and who accepted the residual risk.
3. The model vendor is a third party with a written boundary: where inference runs, what is logged, and what they may retain.
4. Access to the system is role-based, and a change to the model or the prompt is an auditable event.

DESC

5. Someone has written whether this entity is a Dubai government entity or a non-government entity DESC has classified as critical. If neither, DESC is not this file.
6. Prompts, documents, and outputs for an in-scope entity stay on infrastructure DESC's rules allow: their own facility, a certified data centre, or a certified cloud.
7. Electronic-security data is not handed to a third party outside the approval path the entity already uses.
8. Monitoring can show whether the platform called an endpoint it was not supposed to call.

PDPL

9. A list exists of which fields in the prompt and the corpus are personal data. Government data, health data, banking and credit data, and free-zone data under its own law are marked out of this list.
10. Personal data does not leave the UAE unless a transfer case in Articles 22 or 23 of the decree is named in writing. A US region is a transfer.
11. Before a high-risk automated decision, an impact assessment exists: purpose, necessity, risks, and the measures that reduce them. A person can review the decision when the data subject asks.
12. A breach of personal data in the prompt, the log, or the output has a named owner and a notification path. The model vendor's status page is not that path.