Cavoukian's Principle: Passiore currently violates Privacy as the Default Setting. The system deploys with insecure configurations by default like world-readable (777) upload directories and unprotected API endpoints that expose user files immediately upon creation. This would force users to actively intervene to secure their data, whereas the principle dictates that privacy must be the baseline condition without requiring user action or technical knowledge.

ENISA Strategy: To apply the Enforce strategy, the system's architecture must technically mandate the security policy. The database configuration should be redesigned to implement the principle of least privilege. Instead of the current setup where the application connects as a user with global ALL PRIVILEGES. The design must enforce strict access controls by using a dedicated database account limited only to essential commands (like SELECT, INSERT). This ensures that even if the application layer is compromised, the privacy policy remains enforced at the data layer.

Solid data pods: It would would significantly improve passoire by decoupling data storage from the application logic. Like nstead of uploading files to a centralised and vulnerable Passiore server, users would store data in their own personal "pods" and grant Passiore granular permission to read specific files. This reverses the data ownership model, ensuring that a breach of the Passiore application does not compromise the entirety of the user base's data.

Reference:
Cavoukian, A. (2009). Privacy by design: The 7 foundational principles - Implementation and mapping of fair information practices. Information & Privacy Commissioner of Ontario. I also ahve the link to the uni can I add that or is it redundant? https://student.cs.uwaterloo.ca/~cs492/papers/7foundationalprinciples_longer.pdf