**Best Practices Checklist: Securing Sensitive Data in RPA and Agentic AI**

**1. Data Handling Principles**

* Only collect and use the **minimum data necessary**.
* Process sensitive data **in memory**—avoid writing to disk.
* Immediately delete or wipe data after task completion.
* Mask or anonymize data whenever possible (e.g., for testing or logging).

**2. Secure Development Standards**

* Follow secure coding guidelines (e.g., OWASP).
* Flag sensitive data handling clearly in code.
* Use strong encryption for data in transit and at rest (TLS 1.2+, AES-256).
* Validate all inputs to avoid injection or manipulation.
* Create evidence that data policies are adhered to whenever Agentic or RPA agents do work.
* Ensure these practices are identified in design documentation for easy reference.

**3. Testing & Validation**

* Simulate real-world scenarios using sanitized or fake data.
* Ensure test environments **mirror production** without using live data.
* Verify that no sensitive data persists after execution.
* Conduct regular **penetration and security tests**.

**4. Code Reviews & Peer Checks**

* Include security checkpoints in all code reviews.
* Confirm that data access is strictly limited and logged.
* Review how the agent/bot handles errors or incomplete data.
* Use config files for code to reference sensitive details related to the work. Avoid hardcoding these details.

**5. Access Control & Auditing**

* Use **role-based access control (RBAC)** for bots and agents.
* Rotate credentials regularly; never hardcode secrets in code.
* Enable audit logging for actions—without storing sensitive data.
* Monitor agent behavior for anomalies (e.g., accessing data outside scope).