PII & Privacy Risk & Mitigation

AWAKEN ENERGY

Risk Description	Likelihood (1 - 5)	Impact Category	Mitigation Strategy
Unauthorised collection of customer data	3	Moderate	Implement strict data collection guidelines and train sales agents on required information.
Improper data entry by sales agents	4	Moderate	Introduce validation checks in Salesforce to minimise data entry errors.
Unsecured local storage of customer data	3	Major	Ensure all data is stored within encrypted AWS storage and prevent local device storage.
Failure to obtain explicit consent	4	Major	Require digital consent capture through Salesforce with clear opt-in processes.
Data retention policy violations	3	Moderate	Establish automated data retention policies to delete outdated information securely.
Unsecured API data transfers	4	Major	Enforce TLS encryption and secure API configurations for all data transmissions.
Unauthorised API access	5	Catastrophic	Implement role-based access controls (RBAC) and API security tokens with MFA.
Excessive data sharing via API	3	Moderate	Restrict API data transfers to only essential customer information.
API misconfigurations leading to data leaks	4	Major	Conduct regular API security audits and implement real-time monitoring.
Third-party data handling risks	3	Moderate	Review third-party agreements and enforce strict data protection clauses.
Unauthorised employee access to PII	4	Major	Apply access control policies to ensure only authorised personnel can access PII.
Former employees retaining system access	3	Major	Revoke system access for employees immediately upon termination or resignation.
Phishing attacks targeting sales reps	4	Major	Conduct phishing awareness training and implement email security filtering.
Weak password practices	5	Major	Mandate strong password policies and implement enforced periodic password updates.
Lack of multi-factor authentication (MFA)	4	Major	Require multi-factor authentication (MFA) for all system access points.
Lost or stolen sales devices	3	Moderate	Enforce device encryption and remote wipe capabilities for lost or stolen devices.
Paper forms with PII left unsecured	2	Minor	Implement a strict no-paper policy and require digital data entry at point of sale.
Data exposure from public Wi-Fi usage	3	Moderate	Require the use of company-approved VPNs when accessing systems remotely.
Non-compliance with Australian Privacy Principles (APPs)	4	Major	Regularly review compliance with Australian Privacy Principles (APPs) and update policies.
Failure to provide data deletion requests	3	Moderate	Provide a structured process for customers to request data deletion and confirm compliance.

AWAKEN ENERGY