ATECH.AI · SEMP Platform

Privacy Policy & Data Processing Agreement

Last updated: 3 September 2026 · Effective: 5 June 2026 (amended 7 July 2026 and 3 September 2026)

This document governs how Atech Sustainability Consultancy Sdn Bhd (ASC) collects, processes, and protects data submitted to the SEMP platform by client organisations, Registered Energy Auditors (REAs), and Registered Energy Managers (REMs).

1. Overview

Atech Sustainability Consultancy Sdn Bhd ("**ASC**", "**we**", "**our**") operates SEMP, the Sustainable Energy Management Program platform ("**Platform**"), accessible at semp.atechsustainability.com. This Privacy Policy describes how we collect, use, store, and protect information provided by our clients, their appointed energy professionals, and platform users, in accordance with Malaysia's Personal Data Protection Act 2010 as amended by the Personal Data Protection (Amendment) Act 2024 ("**PDPA**").

By accessing or using the Platform, you agree to the practices described in this Policy. If you are accessing the Platform on behalf of a client organisation, you represent that you are authorised to bind that organisation to these terms.

This Policy applies to all users of the Platform, including Registered Energy Auditors (REAs), Registered Energy Managers (REMs), ASC staff, and client organisation users with view-only or operational access.

2. Our Roles Under the PDPA

The Platform handles two kinds of data, and ASC's role differs for each:

Data controller: platform account data

For the personal data of platform users themselves (names, email addresses, roles, professional registration details, and the records of their activity on the Platform), ASC determines the purposes and means of processing and is the **data controller**.

Data processor: Client Data

For building, energy, and audit information submitted by or for a client organisation ("**Client Data**"), including any personal data contained in it such as contact persons or names appearing on utility accounts, the client organisation is the data controller and ASC acts as its **data processor**. In that capacity ASC processes Client Data only to provide the Platform and on the client's instructions, applies the security measures in Section 8, engages only the sub-processors listed in Section 5 under written data processing terms, assists the client with data subject requests concerning Client Data, notifies the client of personal data breaches as set out in Section 9, and returns or deletes Client Data at the end of the engagement as set out in Section 7.

Client Data may be submitted by the client's own personnel, by ASC staff on the client's behalf, or by a duly appointed REA or REM ("**Appointee**") acting under professional appointment. Regardless of who uploads it, Client Data is deemed provided by, and remains the responsibility of, the client organisation.

3. Data We Collect

We process two categories of data: **Personal Data** (relating to identifiable individuals) and **Client Data** (building and energy information).

CATEGORY	EXAMPLES	CLASSIFICATION
User account data	Name, preferred name, email address, role, organisation, sign-in timestamps. Passwords are held only by our authentication provider in hashed form.	Internal
Professional credentials (REA/REM)	Professional registration number, registration type, certificate document, certificate expiry date, and verification status	Internal
Client contact details	Contact person name, designation, email address, and phone number recorded for each client organisation; nominated contact emails for clients using the shared intake folder	Internal
Building identity data	Building name, address, GFA, occupancy type, state	Confidential
Utility & energy data	TNB bills (account number, kWh, MD, PF, cost), baseline consumption, load profiles	Client Confidential
Equipment data	Asset registers, nameplate data, measured kW readings	Client Confidential
Audit outputs	ESM recommendations, M&V plans, bill verification records, regression analyses, reports	Client Confidential

CATEGORY	EXAMPLES	CLASSIFICATION
Raw source files	Uploaded PDFs, scanned utility bills, and Excel files, including the original copy of each bill retained as audit evidence	Client Confidential
Support requests	Ticket subject, description, comments, and attachments; messages sent through the Support form	Internal
AI interaction metadata	Feature name, model used, token counts, duration, and status; no prompt or response content is retained	Internal
Security & audit logs	Actor, action, target, and timestamp of administrative and data actions; security events additionally record IP address, browser user agent, and request path	Internal
Error & diagnostic logs	Stack traces and request metadata, with cookies, request bodies, and user identifiers removed before transmission (via Sentry)	Internal

We do not collect sensitive personal data such as health records, biometric data, government-issued identification numbers, or financial account credentials, and the Platform has no fields for them. You must not upload such data to the Platform.

4. How We Use Your Data

We process data **solely** for the following purposes:

- ✓ Providing the Platform and its energy audit, ESM recommendation, bill verification, and reporting features
- ✓ Extracting data from uploaded utility bills, spreadsheets, and documents so that it can be reviewed and saved by a user
- ✓ Generating AI-assisted energy saving measure recommendations and draft audit report narratives
- ✓ Calculating energy benchmarks (BEI/EUI) against MS 1525:2019 and SEDA requirements
- ✓ Checking professional registrations at sign-up and monitoring certificate expiry, so that only eligible professionals verify Client Data
- ✓ Running automated data-integrity checks on building records to support the accuracy of Client Data (see 4.1 below)
- ✓ Receiving client documents through the optional shared intake folder, and issuing receipts and reminders for it
- ✓ Sending operational emails: registration verification, approvals, reminders, digests, and support ticket updates
- ✓ Maintaining platform security, including security event logging, performance monitoring, and error diagnostics

✓ Responding to and tracking support requests from authorised users

We will **not** use Client Data to train AI models, sell data to third parties, or include your data in aggregated industry benchmarks without your explicit written consent.

4.1 Automated Processing Transparency

The Platform uses two distinct kinds of automated processing, and we distinguish them deliberately:

Deterministic checks (not AI)

A rules engine (the "Virtual Energy Manager") checks each building's records nightly for data-quality and consistency issues, for example missing utility bills or inconsistent figures. Data-health checks run when bills are entered, and documents received through the shared intake folder are classified by their content using fixed rules. These checks apply **fixed, deterministic rules**; they do not use AI or machine learning, do not profile individuals, and make no automated decisions about any person. Each finding must be reviewed by a human user: it is either acknowledged or dismissed with a typed reason, which is retained as evidence. This monitoring exists to support the accuracy of Client Data, a core PDPA principle.

AI-assisted features (always subject to human review)

Document parsing suggestions, the chat assistant, draft ESM and report narrative text, and the extraction of registration details from certificates uploaded at sign-up use the AI models listed in Section 5. AI output is always a **draft or suggestion**: AI never writes directly to Client Data. Saving parsed bill data, approving ESMs, generating reports, and approving a professional's registration are actions taken by a human user. Documents received through the shared intake folder are processed with fixed rules only and are not sent to any AI service.

5. Sub-Processors

ASC engages the following sub-processors. Each is bound by written data processing terms consistent with this Policy. We will give clients at least **14 days' notice** of any addition or replacement by updating this page and emailing the client's designated contact.

SUB-PROCESSOR	ROLE	DATA TOUCHED	LOCATION
Supabase, Inc. (USA)	Database hosting, user authentication, and file storage	Persistent: all Client Data, account data, uploaded files, and logs	AWS ap-southeast-1 (Singapore)

SUB-PROCESSOR	ROLE	DATA TOUCHED	LOCATION
Vercel, Inc. (USA)	Application hosting	Request routing and session checks on the edge network; application functions handle data in memory for the duration of a request, with no persistent storage	Functions: Singapore (sin1); edge network: location nearest the user
Microsoft Corporation (Microsoft 365)	Business email and document collaboration	Messages sent through the Support form and system digests received in ASC's shared mailbox (sender name, email address, message content, file names and statuses); for clients who elect to use the shared intake folder, the documents they place in their own folder	Microsoft 365 data-centre geography assigned to ASC's Malaysian tenant
Alibaba Cloud (Singapore), Model Studio / DashScope International	AI models (Qwen): extraction of data from utility bills, spreadsheets, and documents; extraction of registration details from professional certificates; draft ESM recommendations and draft report narratives	Transient: document images or text extracts sent for inference only; inputs are not used for model training under the provider's product terms	Singapore endpoint
Anthropic, PBC (USA)	AI models (Claude): chat assistant, ESM review, Excel bill import, and spreadsheet column mapping	Transient: data extracts sent for inference only; not used for model training	United States

SUB-PROCESSOR	ROLE	DATA TOUCHED	LOCATION
Resend, Inc. (USA)	Transactional email delivery from noreply@atechsustainability.com: verification, notifications, receipts, and digests	Recipient name, email address, and message content at delivery time	United States
Sentry (Functional Software, Inc., USA)	Application error monitoring	Error reports and request metadata, with cookies, request bodies, and user identifiers removed before transmission; 90-day retention	United States

Transient processing by AI sub-processors involves transmission of specific data extracts for inference only; the Platform does not instruct those providers to store Client Data, and their handling of in-flight data is governed by their respective API terms. On our own systems, AI calls are logged as **metadata only** (feature, model, token counts, duration, and status), with no raw prompt or response content retained in those logs.

6. Data Residency & Cross-Border Transfers

All Client Data and account data is stored at rest within **AWS ap-southeast-1 (Singapore)**. Application functions that read or write that data run in Vercel's **Singapore region** and hold data in memory only for the duration of a request. No persistent storage of Client Data occurs outside Singapore.

The following processing takes place outside Malaysia, each under written data processing terms with the recipient:

- **Singapore**: persistent storage, application functions, and Qwen model inference
- **United States**: Claude model inference, transactional email delivery, and error diagnostics (identifiers removed)
- **Microsoft 365**: email and shared-folder content, in the data-centre geography assigned to ASC's Malaysian tenant

These transfers are made in accordance with section 129 of the PDPA: to jurisdictions whose law provides protection comparable to the PDPA, and with the consent of each user, which is recorded when the user accepts this Policy at registration. ASC does not transfer Client Data to any other jurisdiction without the client's prior written consent.

Singapore Hosting
AWS ap-southeast-1 is geographically proximate to Malaysia and is subject to Singapore's Personal Data Protection Act 2012, which provides a standard of protection comparable to Malaysia's PDPA.

7. Data Retention & Deletion

DATA TYPE	RETENTION PERIOD	BASIS
Active Client Data	Duration of the client engagement; deleted or anonymised within 30 days of the client's written request after termination	Contractual
Audit reports, ESMs, and verification records	7 years after audit completion	EECA 2024 record-keeping
Original utility bills and source files	Retained alongside the audit records they evidence, for the same period	EECA 2024 audit evidence
User account data	Removed when an administrator terminates the account; a professional's certificate file is deleted at the same time	Contractual
Support tickets and attachments	Duration of the client engagement; removed with Client Data on termination	Operational
Intake staging data	Purged automatically 30 days after a batch is approved or rejected	Operational
Unsaved browser drafts	Expire automatically after 14 days, on the user's own device	Operational
AI interaction metadata	Retained for service monitoring and cost control; contains no prompt or response content	Operational
Security and audit logs	Minimum of 12 months, as an accountability and investigation record	PDPA accountability
Error logs (Sentry)	90 days	Operational

Upon written request following the end of an engagement, ASC will return, delete, or anonymise Client Data within **30 days** and confirm completion in writing, except where:

- Retention is required by applicable Malaysian law (EECA 2024, PDPA)

- Data is held in our database provider's backup copies, which are overwritten on the provider's standard rotation
- Data forms part of aggregated, de-identified platform statistics that cannot be traced back to you

8. Security Measures

ASC implements the following technical and organisational measures, representing our current standard practice. Security measures are updated periodically and do not constitute a guarantee against all possible security incidents.

Need-to-know access, enforced at the database layer

Every energy professional (REA, REM, or energy manager) and every client user can access **only the buildings assigned to them** by a platform administrator. This building-scoped access control is enforced by database Row Level Security policies at the database layer, not merely in the user interface, and applies equally to dashboards, automated data-integrity insights, support tickets, and the chat assistant's context. Assignments are granted and revoked by platform administrators, and administrator actions are recorded in the audit trail. Cross-client access is limited to ASC staff with a legitimate operational need.

TECHNICAL

- AES-256 encryption at rest
- TLS 1.2 or higher encryption in transit, with HTTP Strict Transport Security enforced
- Role-based access control with administrator-granted, per-building permissions
- Row Level Security policies on data tables, scoped to assigned buildings
- Uploaded files held in access-controlled storage separate from the database; original bills, certificates, and support attachments are served only through short-lived signed links issued after an access check
- Server-side validation of all file uploads (file type allowlists and size limits)
- Rate limiting on public endpoints (registration, lookups)
- Automatic sign-out after 30 minutes of inactivity
- Security event logging: sign-in outcomes, access denials, data exports, and certificate views recorded with actor, IP address, user agent, and timestamp
- Privileged credentials held server-side only and never exposed to the browser; scheduled jobs and inbound webhooks authenticated with server-held secrets
- Shared intake folder integration uses a certificate-based application identity scoped to a single site; every file received is hashed (SHA-256) for integrity and duplicate detection
- User identifiers, cookies, and request bodies stripped from error reports before they leave the platform
- Security response headers (HSTS, frame, content-type, and referrer protections)

- AI spend caps and provider health alerting

ORGANISATIONAL

- Verified email required before any account is considered for approval
- Accounts remain disabled until explicitly approved by a platform administrator
- REA/REM registrations require certification documents, reviewed before approval; duplicate registration numbers are rejected
- Bill verification is restricted to professionals holding a current registration and an assignment to the building concerned
- Access limited to staff with a legitimate need
- Sub-processor due diligence with written data processing terms
- Documented incident response and data subject request procedures, owned by the Data Protection Officer
- Periodic independent security reviews of the codebase and database access policies
- Data classification applied to all data types (see Section 3)

AUDIT TRAIL

- Administrative and data actions logged with actor, action, target, and timestamp, including field-level before-and-after values for edits
- Building access grants and revocations by administrators logged
- Bill verification records: which professional verified which bill, and when
- Every file received through the shared intake folder recorded with its hash, outcome, and the approving administrator
- Document acknowledgements recorded (who acknowledged, and when)
- Dismissing an automated data-integrity finding requires a typed justification, retained as evidence

DATA INTEGRITY

- Automated nightly data-integrity monitoring of every building (deterministic rules, see Section 4.1)
- Intake checks on every bill: duplicate detection, billing-period and account consistency, and a confidence score on extracted figures
- Every saved bill can be viewed side by side with its original document
- Findings carry a human acknowledge/dismiss lifecycle with recorded outcomes
- Human review gates on AI-assisted outputs: parsed bills, ESMs, and reports require user action

9. Incident Response

ASC maintains a documented personal data breach response procedure, owned by our Data Protection Officer, with defined roles, severity classification, and notification decision steps. Our commitments follow the PDPA breach notification regime introduced by the 2024 Amendment:

- **Where ASC is the data controller** (platform account data), ASC will notify the Personal Data Protection Commissioner as soon as practicable and in any event within **72 hours** of becoming aware of a personal data breach, and will notify affected individuals without unnecessary delay, and in any event within **7 days**, where the breach is likely to cause them significant harm.
- **Where ASC is the data processor** (Client Data), ASC will notify the affected client without undue delay and in any event within **72 hours** of becoming aware of a personal data breach affecting that client's data, so that the client can meet its own obligations as data controller. ASC will cooperate with the client's assessment and any notification the client makes.

Notifications will include:

- Nature of the breach and the categories of data affected
- Estimated number of data subjects and records involved
- Likely consequences
- Measures taken or proposed to contain and remediate the breach
- Contact details of our Data Protection Officer

Where the full extent of a breach cannot be established within the initial window, ASC will provide an initial notification with the information available and supplement it as further details are confirmed. Where a breach originates at a sub-processor, ASC's awareness begins when the sub-processor notifies us, and ASC remains responsible for notifying the client.

Incidents arising from the use of a client's or an Appointee's own credentials, or from their own actions, are investigated and handled in cooperation with the client.

10. Your Rights Under the PDPA

Under Malaysia's Personal Data Protection Act 2010, as amended in 2024, you have the following rights with respect to your Personal Data:

→ **Right of Access**
Request a copy of the Personal Data we hold about you.

→ **Right of Correction**
Request correction of inaccurate or incomplete Personal Data.

→ **Right to Data Portability**
Receive the Personal Data you have provided to us in a structured, commonly used, machine-readable format, as introduced by the 2024 Amendment.

→ **Right to Withdraw Consent**
Withdraw consent for processing at any time, subject to legal or contractual obligations. Withdrawing consent to AI-assisted processing means those features can no longer be used for your uploads.

→ **Right to Deletion**
Request deletion of your Personal Data, subject to retention obligations under EECA 2024 and the PDPA retention principle (data is not kept longer than necessary).

→ **Right to Prevent Processing**
Require us to cease processing likely to cause damage or distress, and to cease processing for direct marketing purposes. ASC does not use Platform data for direct marketing.

Requests are handled under a documented procedure. We verify the identity of the requester before acting, and the Platform's audit trail (Section 8) allows us to identify what data we hold about you and how it has been processed. Requests concerning personal data contained in Client Data are referred to the client organisation as data controller, and we assist it in responding.

To exercise any of these rights, contact our Data Protection Officer at kentphang@atechnologies.com.my. We will acknowledge your request on receipt and respond within 21 days.

11. Cookies & Local Storage

The Platform uses **strictly necessary cookies only**. Our authentication provider sets session cookies to keep you signed in and to refresh your session automatically; they are removed when you sign out. We do not use advertising, tracking, or analytics cookies.

- **Browser local storage** holds your display theme preference and any unsaved upload draft, which expires after 14 days. This data stays on your own device.
- **Error monitoring** runs in the browser to report application errors. It does not set cookies and does not transmit user identifiers.

12. AI Output Disclaimer

> Platform Outputs, including ESM recommendations, energy audit narratives, regression analyses, and benchmarks, are provided for **informational and decision-support purposes only**. They do not constitute professional engineering, legal, or financial advice.

Platform Outputs fall into two categories, and users should understand the distinction:

- **AI-generated content**: document parsing suggestions, chat assistant responses, and draft ESM and report narrative text. These are drafts and suggestions only, are **always subject to human verification** before being saved or relied upon, and chat responses carry an in-product disclaimer. AI never writes directly to Client Data.
- **Deterministic outputs**: benchmark calculations (BEI/EUI), regression analyses, and data-integrity findings from the rules engine described in Section 4.1. These are produced by fixed formulas and rules, not AI models.

For transparency: our systems log AI usage as metadata only (feature, model, token counts, duration, and status). Raw prompt and response content is not retained in those logs.

The professional responsibility for all energy audit conclusions, certifications, and submissions to SEDA Malaysia or any regulatory authority rests solely with the appointed REA or REM and the client organisation. ASC accepts no liability for decisions made in reliance on Platform Outputs without independent professional verification.

13. Limitation of Liability

To the maximum extent permitted by Malaysian law:

- ASC shall not be liable for loss of profit, revenue, business, or opportunity
- ASC shall not be liable for loss of data caused by the client's or an Appointee's own actions
- ASC shall not be liable for indirect, consequential, special, or punitive damages
- ASC shall not be liable for any loss arising from reliance on Platform Outputs for professional, regulatory, or investment decisions

ASC's total aggregate liability under this Policy shall not exceed the **total fees paid by the client in the three months immediately preceding the event giving rise to the claim**.

14. Contact Us

For privacy enquiries, data subject requests, or to request a copy of our standalone Data Processing Agreement and sub-processor register, contact:

Company	**Atech Sustainability Consultancy Sdn Bhd (ASC)**
DPO	Kent Phang, Data Protection Officer
Email	kentphang@atechnologies.com.my
Platform	SEMP, semp.atechsustainability.com
Governing law	Malaysia: Personal Data Protection Act 2010 (as amended 2024)