ATECH · ESG Platform

Privacy Policy & Data Processing Agreement

Last updated: 9 September 2026 · Effective: 9 September 2026 · Version 1.0

This document governs how Atech Sustainability Consultancy Sdn Bhd (ASC) collects, processes and protects data submitted to the Atech ESG Platform by client organisations and by the consultants who work on their behalf.

1. Overview

Atech Sustainability Consultancy Sdn Bhd ("**ASC**", "**we**", "**our**") operates the Atech ESG Platform ("**Platform**"), accessible at esg.atechsustainability.com. The Platform supports ESG materiality assessment, policy and activity tracking, evidence management, sustainability data collection and the preparation of declarations to ESG rating standards such as EcoVadis and the Bursa Malaysia Simplified ESG Disclosure Guide. This Policy describes how we collect, use, store and protect information provided by our clients 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: ASC staff, associate consultants engaged by ASC, and any client organisation representative who is given an account.

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, access approvals and the records of their actions on the Platform), ASC determines the purposes and means of processing and is the **data controller**.

Data processor: Client Data

For the ESG information submitted by or for a client organisation ("**Client Data**"): materiality assessments, policies, activities, evidence documents, sustainability and energy data, declarations, scores and reports, including any personal data contained in it, such as employee names in training records, signatories of policies, stakeholder names, or supplier contacts, 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 its consultancy service 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 is normally entered and uploaded by ASC consultants on the client's behalf under the engagement letter, from documents and figures the client supplies. 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** (ESG, sustainability and energy information about a company).

Category	Examples	Classification
User account data	Name, email address, role (member or superadmin), access status and the superadmin who approved it, last sign-in time. Passwords are held only by our authentication provider in hashed form; the Platform never stores them.	Internal
Client identity data	Company name, industry classification, number of employees, assessment scope, rating deadline, sites and countries, notes, and the operations profile (premises, fleet, processes, procurement)	Confidential
Materiality records	Context answers, topic screening decisions and reasons, impact and financial ratings, stakeholder names, groups, influence and interest ratings, engagement events, and uploaded survey responses	Client Confidential
Policies and activities	Policy text, versions, issue and expiry dates, targets, approval records; logged activities with dates, sites and descriptions	Client Confidential
Evidence documents	Uploaded PDFs such as policies, procedures, training records, certificates, audit reports and signed declarations, which may contain names of employees, signatories or suppliers; the metadata extracted from them	Client Confidential
Sustainability data	Energy, fuel, water, waste and travel records, utility figures, uploaded workbooks and ledgers, emission factors applied, calculated emissions and intensities	Client Confidential
Declarations and scores	Options claimed against a rating standard, comments, theme weights, simulated scores and yearly score snapshots, action plans, and exported PDF, DOCX and Excel reports	Client Confidential
AI run records	The task requested, the role used, the draft produced, and who approved or rejected it; the structured proposals produced when a document or workbook is analysed	Client Confidential

Platform request logs	Request path, status, timestamp and connecting IP address, held briefly by the hosting provider for operations and security	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. Evidence documents must not contain such data: redact medical details from health and safety records, and identity numbers from training or HR records, before uploading.

4. How We Use Your Data

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

- Providing the Platform and its materiality, policy, activity, evidence, sustainability data, declaration, rating and reporting features
- Reading uploaded documents and workbooks so that their details can be pre-filled for a consultant to review and confirm
- Generating AI-assisted drafts: policy wording, materiality shortlists, industry-specific activity suggestions, disclosure narratives and pre-audit reviews
- Simulating scores against the selected rating standard, and calculating greenhouse gas emissions and intensities from the recorded data
- Checking that only confirmed and approved accounts can log in, and recording who approved each account
- Sending operational emails: account confirmation and password reset only
- Maintaining platform security and diagnosing faults

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 rules (not AI)

Materiality screening, the scoring engine, emission calculations, evidence validity and coverage checks, and the status shown on each tab apply **fixed, documented rules**: for example, a topic is shortlisted because of an answer given in Step 1, or an indicator is deactivated because the company holds no certifications. They do not use machine learning, do not profile individuals, and make no automated decision about any person. Every screening decision keeps its reason and can be changed by a consultant.

AI-assisted features (always subject to human review)

Smart upload of evidence, workbook and questionnaire imports, emission factor checks, stakeholder survey reading, the AI Assist subagents and "Draft fix with AI" use the AI models listed in Section 5. AI output is always a **draft or suggestion**: AI never writes directly to Client Data. Filing a document, saving imported figures, applying a factor change, accepting a suggested activity, and approving a draft are actions taken by a consultant, and the Platform records who took them.

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, file storage, and delivery of account confirmation and password reset emails	Persistent: all Client Data, account data and uploaded files; recipient address and link for authentication emails	AWS ap-southeast-1 (Singapore); email delivery through the provider's mail service
Vercel, Inc. (USA)	Application hosting	Application functions handle data in memory for the duration of a request, with no persistent storage; request logs held for a short rolling period	Functions: Singapore (sin1); edge network: location nearest the user
Anthropic, PBC (USA)	AI models (Claude): document and workbook analysis, questionnaire reconciliation, emission factor checks, drafts and reviews	Transient: document text or images and data extracts sent for inference only; not used for model training under the provider's commercial terms	United States

Transient processing by the AI sub-processor involves transmission of specific data extracts for inference only; the Platform does not instruct the provider to store Client Data, and its handling of in-flight data is governed by its API terms. On our own systems, each AI run is recorded with its task, the draft produced and the consultant's decision, so that every AI-assisted change to Client Data can be traced.

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, file storage and application functions
- **United States**: Claude model inference and delivery of authentication emails

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
Submitted declarations, score snapshots and the evidence behind them	7 years after the reporting year, as the record of what was declared to a rating body, unless the client requests earlier deletion	Contractual; rating-body audit
User account data	Removed when a superadmin removes the account; the login held by the authentication provider is deleted on request	Contractual
AI run records and document analyses	Kept with the Client Data they relate to; discarded analyses are deleted immediately	Operational
Database backups	Daily copies held by the database provider on a rolling basis, currently seven days	Operational
Platform request logs	Short rolling period held by the hosting provider, currently up to one day	Operational
Browser storage	Display theme preference and recently viewed page snapshots, on the user's own device until browser data is cleared	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
- 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.

Who can see Client Data. Every account is held by an ASC consultant or associate, or by a client representative approved by an ASC superadmin. Accounts become active only after the email address is confirmed and, for addresses outside ASC's own domains, after a superadmin approves the request. Approved users work across ASC's client portfolio and can open every client workspace; there are no client-side self-service logins in this version. Superadmins can remove a user's access at any time, and every approval and removal is recorded with who made it and when.

Technical

- AES-256 encryption at rest for the database, backups and stored files

- TLS 1.2 or higher encryption in transit, with HTTP Strict Transport Security enforced by the hosting provider
- Passwords never stored by the Platform; authentication handled by Supabase Auth with hashed credentials, email confirmation and expiring reset links
- Uploaded files held in private, access-controlled storage separate from the database; documents are served only through signed links that expire after 10 minutes and are issued to logged-in users
- Browser uploads go directly to storage over TLS through short-lived signed upload links; the application server never holds a copy
- Server-side validation of uploads: evidence must be a PDF of at most 20 MB, and workbooks are checked before any figures are proposed
- Secure, HTTP-only session cookies and CSRF protection on every form
- Privileged credentials, API keys and database connection strings held server-side as environment variables and never exposed to the browser
- Content-type, referrer and clickjacking protections in every response
- AI requests time-limited, and each run recorded with its task, output and reviewer decision

Organisational

- Confirmed email required before any account is considered; accounts outside ASC's own email domains remain blocked until a superadmin approves them
- Superadmin role granted by company email domain; access reviewed and removed on the Access page when a consultant leaves an engagement
- Every AI-assisted output reviewed by a consultant before it becomes Client Data
- Sub-processor due diligence with written data processing terms
- Documented incident response and data subject request procedures, owned by the Data Protection Officer
- Hosting locations and AI processing disclosed in client engagement letters
- Data classification applied to all data types (see Section 3)

Audit trail

- Policy approvals, materiality screening confirmations and access decisions recorded with the user and time
- Document uploads, workbook imports and AI runs recorded with the consultant who started them and the one who confirmed, approved or rejected the result
- Emission factor verifications recorded with the verifying user; proposed factor changes kept with their source citations until applied or dismissed
- Yearly score snapshots dated and kept as the record of each reporting year

Data integrity

- Evidence validity tracked by issue and expiry dates; expired or undated documents are flagged and excluded from the score
- Coverage checks show which material topics lack a policy, an activity, evidence or a KPI

- Human confirmation gates on every AI-assisted output: filed documents, imported figures, factor changes, suggested activities and drafts all 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 representative'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 documents.

Right to deletion. Request deletion of your Personal Data, subject to the retention commitments in Section 7 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 records (Section 8) allow 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**: a session cookie that keeps you signed in and a token that protects forms against forgery. The session cookie is removed when you log out and expires on its own after two weeks. We do not use advertising, tracking or analytics cookies.

- **Browser local storage** holds your display theme preference and snapshots of recently viewed pages used to make navigation faster. This data stays on your own device and is removed when you clear your browser data.
- **No third-party scripts** run in the browser: all page assets are served by the Platform itself.

12. AI Output and Score Disclaimer

Platform outputs, including simulated ESG scores, gap analyses, action plans, drafted policies and disclosure narratives, are provided for **informational and decision-support purposes only**. They do not constitute professional, legal or financial advice, and a simulated score is not an official rating from any rating body.

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

- **AI-generated content**: document and workbook analyses, suggested activities, drafted policies, narratives and reviews. These are drafts and suggestions only, are **always subject to human verification** before being saved or relied upon, and AI never writes directly to Client Data.
- **Deterministic outputs**: simulated scores, theme scores, emission calculations, validity and coverage checks. These are produced by fixed formulas and rules, not AI models, and the rating body's own assessment may differ.

The responsibility for what is declared to a rating body, regulator or stakeholder rests solely with the client organisation and the consultant who prepares the submission. ASC accepts no liability for decisions made in reliance on Platform outputs without independent 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 its representative'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, including any difference between a simulated score and a rating body's assessment

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	Atech ESG Platform, esg.atechsustainability.com
Governing law	Malaysia: Personal Data Protection Act 2010 (as amended 2024)

© 2026 Atech Sustainability Consultancy Sdn Bhd (ASC). All rights reserved. · Atech ESG Platform · Governed by Malaysian law