

AIDER MASTER PRIVACY POLICY

MYAIDER HOLDING SDN. BHD.

Company Registration No. 202301007378

Version 1.0

Last Updated: 4 September 2026

Master privacy notice covering Customers, Drivers, Corporate Clients, Merchants, SME Partners, Vehicle Owners, Website/App Users and other Aider ecosystem participants.

Publication Status:

This document is a comprehensive master policy intended for adoption and publication after final operational verification and legal review. Once adopted and published, it is intended to supersede the Privacy Policy dated 17 December 2025.

IMPORTANT NOTICE

This Privacy Policy is a notice explaining Aider's processing of personal data.

It is not intended to operate as blanket consent.

Where consent is required by law, app-store rules, device permissions or the nature of a feature, Aider will seek that consent separately and record it as appropriate.

1. WHO WE ARE AND PURPOSE OF THIS POLICY

This Master Privacy Policy ("Policy") explains how **MYAIDER HOLDING SDN. BHD.** (Company Registration No. 202301007378) ("Aider", "MyAider", "we", "our" or "us") collects, receives, records, organises, stores, uses, analyses, shares, transfers, discloses, retains, secures and deletes personal data in connection with the Aider Driver Platform and related websites, mobile applications, portals, communications, support channels, programmes and ecosystem services (collectively, the "Platform").

Aider operates a technology-enabled mobility and operational support platform that facilitates driver-service arrangements and ecosystem collaborations among users, independent drivers/service providers, merchants, SME operators, vehicle owners, corporate clients and business partners.

The Platform may include:

- Driver by Distance;
- Driver by Hour;
- Driver-With-Vehicle;
- Commercial Vehicle Driver;
- Executive Chauffeur;
- Scheduled Commute;
- Corporate/Contract Driver;
- Cross-border Driver;
- prepaid hours;
- merchant/referral programmes;
- car-owner features;
- vouchers;
- rewards;
- cashback;
- loyalty;
- promotional campaigns; and
- future ecosystem services.

This Policy should be read together with the current **Aider Platform Terms, Ecosystem & Operational Policy** and any feature-specific notice shown at the point of collection.

The Terms govern use of the Platform and service relationships; this Policy governs personal-data processing.

If a specific privacy notice gives more detailed information for a feature, that specific notice applies to that feature to the extent of the additional detail.

2. WHO THIS POLICY COVERS

This Policy is intended to cover personal data relating to the following categories of individuals, whether they hold an account or interact with Aider through another authorised person:

2.1 Customers and Users

Customers and prospective customers, including passengers and authorised representatives where relevant.

Data may include identity/contact information, bookings, locations, vehicle details, payments, communications, ratings, support information and incident evidence.

Such information may be used for booking fulfilment, driver matching, payment/refunds, safety and dispute handling.

Assigned drivers receive only information reasonably needed to perform the booking.

2.2 Drivers and Service Providers

Drivers and prospective drivers operating as independent service providers unless a separate written arrangement states otherwise.

Data may include identity information, licence/eligibility information, profile information, bank/payout data, availability, booking activity, GPS information, ratings, safety/fatigue indicators, complaints and verification records.

Such information may be used for onboarding, matching/dispatch, payout, safety, service quality, fraud prevention and compliance.

Customers may see driver profile, verification and booking-relevant information.

2.3 Corporate Clients, Administrators and Authorised Users

Corporate clients, corporate administrators, employees or authorised users using a corporate account, package or benefit.

Data may include organisation information, authorised-user details, booking/usage records, allocations, invoices, policy controls and support records.

Such information may be used for corporate account administration, allocation of hours or benefits, billing and policy enforcement.

Corporate administrators may see authorised-user usage and charges as configured.

2.4 Merchants, SME and Referral Partners

Merchants, SME operators, referral partners, workshops, logistics or hospitality operators, event organisers and other ecosystem or business partners.

Data may include business/contact information, referral codes, campaign attribution, commission or incentive records, settlement data and compliance records.

Such information may be used for partner administration, referral verification, commissions, fraud prevention and reporting.

Full trip details are not provided merely because a referral occurred unless necessary, authorised or legally required.

2.5 Vehicle Owners and Car-Owner Participants

Vehicle owners, authorised vehicle representatives and persons whose information is contained in vehicle-service or inspection records.

Data may include vehicle identifiers, maintenance or inspection history, mileage, photographs, servicing information and ownership or authorisation information.

Such information may be used for vehicle-related ecosystem features, operational verification, safety, service records and disputes.

2.6 Website Visitors, Prospective Users and Support Contacts

Website visitors, app users, recipients of promotions, people who contact support, complainants, witnesses, claimants and other persons whose data is reasonably involved in a booking, safety event, dispute or investigation.

Data may include device/browser information, cookies where used, enquiry information, campaign interactions and communications.

2.7 Other Ecosystem Participants

Any other person whose personal data is processed in connection with an Aider service, programme, campaign or ecosystem feature.

3. AIDER'S DATA-PROTECTION ROLE

For most Platform operations, Aider determines the purposes and means of processing personal data and acts as a data controller, or equivalent concept under applicable law.

In some corporate, partner or outsourced arrangements, Aider may process specified data on another organisation's documented instructions, or both parties may act as separate controllers for their respective purposes.

The applicable contract or data-processing arrangement may further allocate responsibilities.

Drivers, merchants, corporate clients, payment providers, insurers and other third parties may independently process personal data for their own lawful purposes.

Their own privacy notices may apply to processing they independently control.

Aider's disclosure of data to such parties remains governed by this Policy and applicable law.

4. PERSONAL DATA WE MAY COLLECT AND PROCESS

4.1 Account, Identity and Contact Data

We may collect:

- name;
- preferred name;
- phone number;
- email address;
- date of birth;
- profile image;
- account identifiers;
- login and authentication records;
- postal or business address where needed;
- language;
- country or region; and
- communication preferences.

4.2 Identity, Eligibility and Verification Data

We may collect:

- NRIC/passport or other identity-document details;
- driving-licence information;
- verification images;
- document validity and expiry information;
- eligibility checks;
- driver onboarding records;
- training and compliance status; and
- other verification information reasonably required for safety, fraud prevention, Platform access or legal obligations.

If Aider introduces biometric verification, biometric data will only be processed with the specific notice, safeguards and consent or other legal basis required by applicable law.

4.3 Customer Booking, Service and Vehicle Data

We may collect:

- pickup and drop-off locations;
- requested times;
- stops;

- booking type;
- service duration;
- special instructions;
- vehicle make, model and registration;
- other relevant vehicle identifiers;
- authorised driver-access information;
- booking changes;
- waiting and cancellation events;
- trip completion status;
- ratings;
- reviews;
- service history; and
- related operational records.

4.4 Driver and Service-Provider Data

We may collect:

- driver profile;
- verification status;
- availability or online status;
- assigned bookings;
- accepted bookings;
- service history;
- ratings;
- customer feedback;
- cancellations;
- arrival/check-in status;
- navigation and trip activity;
- payout and bank details;
- incentive and commission records;
- compliance actions;
- complaints;
- disciplinary or restriction records;
- safety indicators;
- fatigue-related indicators where collected; and
- records reasonably required to establish service eligibility and Platform integrity.

4.5 Location, Route, Trip and Operational Telemetry

We may collect:

- approximate location;
- precise device location;
- pickup location;
- arrival location;
- GPS route;
- trip progress;
- timestamps;
- stops;
- location accuracy; and
- other operational telemetry reasonably required for matching, dispatch, navigation, ETA, safety monitoring, arrival or waiting verification, route-anomaly review, dispute evidence, fraud prevention or service quality.

Depending on the role and feature, location may be collected while the app is in use and, where justified and separately disclosed, in the background.

4.6 Vehicle-Condition, Inspection and Incident Evidence

We may collect:

- exterior vehicle photographs;
- interior vehicle photographs;
- dashboard or mileage images;
- visible scratches or dents;
- tyre condition;
- fuel level;
- battery level;
- timestamps;
- GPS verification;
- accident or incident reports;
- driver statements;
- customer statements;
- insurance-related documentation; and
- other evidence reasonably collected before, during or after a booking.

These records may incidentally contain people, number plates, surroundings or other personal information.

4.7 Communications, Support and Dispute Data

We may collect:

- in-app messages;
- support chats;
- emails;
- WhatsApp or other official-channel communications;
- call-attempt records;
- call metadata;
- support-call recordings where the call is expressly recorded with appropriate notice;
- complaint submissions;
- dispute submissions;
- attachments;
- customer-service notes;
- investigation records; and
- investigation outcomes.

Aider may preserve relevant communications as evidence where a dispute, safety issue, fraud concern, chargeback or legal matter exists.

4.8 Payment, Financial, Payout and Transaction Data

We may collect or process:

- payment method tokens;
- masked payment details;
- transaction references;
- charges;
- deposits;
- refunds;
- credits;
- vouchers;
- prepaid balances;
- invoices;
- receipts;
- chargebacks;
- referral records;
- commission records;
- bank and payout details for drivers or partners; and
- accounting records.

Full card credentials are generally processed by payment providers and are not intended to be stored by Aider unless a specific compliant payment arrangement requires otherwise.

4.9 Device, App, Website and Security Data

We may collect:

- IP address;
- device identifiers;
- operating system;
- app version;
- network information;
- browser information;
- push-notification tokens;
- session and login records;
- crash logs;
- diagnostics;
- app interactions;
- timestamps;
- cookies or similar technologies where used;
- security events;
- abuse signals; and
- audit logs.

4.10 Corporate, Merchant, SME, Referral and Ecosystem Data

We may collect:

- organisation information;
- business-contact details;
- company identifiers;
- authorised-user lists;
- corporate allocations;
- package usage;
- billing records;
- merchant or referral codes;
- campaign attribution;
- commissions;
- partner-settlement information;
- service eligibility;
- programme participation; and
- compliance and fraud records.

Aider may receive employee or authorised-user details from a corporate client or partner that is authorised to provide them.

4.11 Marketing, Promotions, Loyalty and CRM Data

We may collect or derive:

- campaign participation;
- voucher usage;
- cashback usage;
- reward usage;
- referrals;
- communication preferences;
- engagement with Aider messages;
- service interests;
- aggregated usage patterns; and
- customer-relationship attributes.

Such information may be used to personalise service communications, measure campaign effectiveness, prevent promotional abuse and, where permitted, provide relevant offers.

4.12 Sensitive or Higher-Risk Data

Certain information may be considered sensitive or higher risk under applicable law, including:

- identity-document information;
- financial information;
- precise location;
- biometric information if ever enabled;
- information regarding alleged offences or fraud; and
- health or safety information voluntarily provided in an emergency or fitness context.

Aider applies additional controls and obtains explicit or other legally required consent where applicable.

5. WHERE PERSONAL DATA COMES FROM

Aider may obtain personal data from:

- you directly through registration, booking, onboarding, forms, support, claims, surveys and communications;
- your device or browser through app functions, permissions, telemetry, security logs, cookies or similar technologies;
- other Platform participants such as customers, drivers, corporate administrators, merchants, vehicle owners, authorised representatives or referral partners;
- payment gateways;
- banks;
- mapping and navigation providers;
- telecommunications providers;
- identity or background-verification providers;
- insurers;
- cloud or hosting providers;
- other service providers;
- publicly available sources;
- regulatory or licensing sources;
- other legally accessible sources where verification, safety, fraud prevention or legal compliance reasonably requires it; and
- system-generated or inferred information such as service status, risk flags, campaign attribution, route anomalies or performance indicators generated from Platform activity.

If you provide personal data about another person, you are responsible for having a lawful basis and, where required, informing that person that their data may be provided to Aider.

Do not provide more third-party data than is necessary.

6. WHY WE PROCESS PERSONAL DATA

We may process personal data for the following purposes, to the extent relevant to your role and the feature you use:

- create, authenticate, maintain and secure accounts;
- manage profiles, preferences and access rights;
- verify identity;
- verify driver eligibility;
- verify licences and documents;
- verify corporate authority;
- verify partner eligibility;
- satisfy compliance requirements;
- receive bookings and service requests;
- match and dispatch bookings;
- manage, modify, complete and record bookings;
- provide navigation;
- verify pickup and arrival;
- provide ETA information;
- monitor route or trip progress;
- facilitate communications;
- provide operational coordination;
- calculate service charges;
- calculate waiting, cancellation and overtime charges;
- calculate taxes;
- calculate discounts;
- calculate credits and other Platform entitlements;
- process payments;
- process payouts;
- process refunds;
- manage chargebacks;
- administer commissions;
- administer credits;
- issue invoices;
- perform accounting and financial reconciliation;
- provide customer support;
- investigate complaints;
- determine disputes;
- preserve and use digital evidence where permitted;
- protect customers, drivers, vehicles, the public and the Platform;
- perform safety monitoring;
- implement fatigue or risk controls;
- handle incidents;

- coordinate emergencies;
- detect, prevent and investigate fraud;
- investigate unauthorised transactions;
- identify promotional abuse;
- identify duplicate accounts;
- investigate off-platform activity;
- identify security incidents;
- investigate policy violations;
- manage corporate packages;
- manage prepaid hours;
- manage merchant and referral programmes;
- administer SME-support programmes;
- administer rewards;
- administer loyalty programmes;
- administer cashback;
- manage future ecosystem features;
- improve functionality;
- improve reliability;
- improve service quality;
- improve user experience;
- improve support operations;
- conduct analytics;
- perform internal planning;
- send service communications;
- send transaction communications;
- send safety and security communications;
- send policy and account communications;
- send other important non-marketing notices;
- send marketing or promotional communications where permitted;
- personalise offers where permitted;
- establish, exercise or defend legal claims;
- cooperate lawfully with insurers and professional advisers;
- cooperate with courts, regulators and police;
- comply with legal and regulatory obligations;
- comply with tax and accounting requirements;
- comply with licensing requirements;
- comply with data-protection obligations;
- respond to lawful law-enforcement requests; and
- support corporate transactions, restructuring, financing, audits or due diligence subject to appropriate confidentiality and legal safeguards.

7. CONSENT, NECESSITY AND OTHER PERMITTED GROUNDS

Aider will obtain consent where consent is required.

Depending on applicable law and context, processing may also be permitted because it is necessary to:

- provide a service you requested;
- administer a contract or account;
- comply with law;
- protect vital interests or safety;
- establish or defend claims;
- prevent fraud or security threats; or
- pursue legitimate business purposes recognised by applicable law.

Some information is mandatory for particular functions.

For example, a booking cannot normally be fulfilled without pickup details, and a driver cannot normally provide services without identity/licence verification and operational location where required.

If mandatory information is not provided, Aider may be unable to:

- create or maintain an account;
- verify eligibility;
- process a booking;
- make a payout;
- investigate a safety matter; or
- provide the relevant feature.

Where processing is optional, we will identify the choice where reasonably practicable.

Withdrawal of consent does not invalidate processing lawfully carried out before withdrawal and may not require deletion of information that Aider must or is permitted to retain for legal, safety, fraud, accounting, dispute or other lawful reasons.

8. LOCATION AND BACKGROUND LOCATION

Location is central to many Aider services.

Customers may provide pickup and drop-off addresses manually or through device location where the feature allows.

Drivers may need to provide precise operational location when:

- online;
- available for bookings;
- assigned to a booking;
- approaching a pickup;
- waiting at a pickup;
- performing a booking; or
- completing other functions for which operational location is reasonably required.

This allows Aider to:

- match drivers and customers;
- dispatch drivers;
- provide navigation;
- verify arrival;
- verify waiting time;
- monitor trip progress;
- provide operational support;
- investigate route anomalies; and
- support safety.

If background location is technically necessary for a driver or safety feature, Aider will use the relevant operating-system permission and any prominent in-app disclosure required by platform rules or law.

Background collection should be limited to the duration and scope reasonably necessary for the disclosed feature.

Location is not intended to be sold for advertising purposes.

9. SAFETY MONITORING, DIGITAL EVIDENCE AND INVESTIGATIONS

The Platform may rely on operational records including:

- booking records;
- GPS tracking;
- driver activity logs;
- communications;
- payment records;
- arrival proof;
- login records;
- IP-address records;
- timestamps;
- vehicle-condition photographs; and
- internal investigation records.

These records may be used to:

- verify arrival;
- determine waiting time;
- investigate service quality;
- investigate accidents;
- investigate vehicle damage;
- investigate unauthorised transactions;
- investigate fraud;
- investigate safety issues;
- respond to chargebacks;
- investigate complaints; and
- determine other disputes.

Aider may preserve or restrict access to relevant evidence where a:

- legal hold;
- open complaint;
- safety incident;
- insurance claim;
- fraud investigation;
- law-enforcement request; or
- other legitimate need

applies.

Information may remain retained even if it is no longer visible in the normal user interface.

Access to investigation material may be limited where disclosure would:

- prejudice an investigation;
- infringe another person's rights;
- expose security controls; or
- otherwise be subject to lawful refusal, restriction or redaction.

10. AUTOMATED SYSTEMS, AI, PROFILING AND HUMAN REVIEW

Aider may use automated or AI-assisted systems to support activities such as:

- driver and customer matching;
- dispatch prioritisation;
- ETA calculations;
- route analysis;
- fraud detection;
- abuse detection;
- account and security alerts;
- promotional eligibility;
- customer relationship management;
- service-quality analysis; and
- operational risk indicators.

Such systems may generate:

- recommendations;
- flags;
- scores;
- segments; or
- predicted outcomes

from Platform data.

Where an automated decision may produce a legal or similarly significant effect on an individual, Aider will apply safeguards required by applicable law.

Unless applicable law permits otherwise with appropriate safeguards, Aider does not intend to rely solely on automated processing for such a decision without meaningful human involvement or review.

Where applicable, an affected person may request information about, or human review of, a significant automated decision through the privacy contact channel.

If third-party AI services are used, Aider will:

- assess the data involved;
- limit disclosure to what is reasonably necessary;
- apply contractual and security controls where available; and
- remain responsible for disclosures required by app-store policies and applicable data-protection law.

11. HOW WE SHARE OR DISCLOSE PERSONAL DATA

Aider may disclose personal data only to the extent reasonably necessary for the stated purposes.

11.1 Customers and Drivers

A customer may receive an assigned driver's:

- name;
- profile photo;
- verification information;
- rating information; and
- service-contact mechanism.

A driver may receive:

- customer or booking identifier;
- pickup location;
- drop-off location;
- relevant vehicle information; and
- special instructions required to perform the service.

11.2 Corporate Clients and Administrators

Information may be disclosed to corporate clients or administrators for:

- corporate-account administration;
- authorised-user management;
- allocation;
- usage management;
- policy controls;
- invoicing; and
- reconciliation.

If you use a corporate benefit, your organisation may be able to see booking, usage and charge information as configured.

11.3 Merchants, SME and Referral Partners

Information may be disclosed for:

- attribution;
- eligibility;
- campaign administration;
- commission verification; and
- partner reporting.

Aider does not intend to provide full trip details merely because a referral occurred unless such disclosure is necessary, authorised or lawful.

11.4 Payment and Financial Providers

Information may be disclosed to:

- payment gateways;
- banks; and
- financial institutions

for payment, payout, refunds, fraud prevention and chargeback handling.

11.5 Technology and Service Providers

Information may be disclosed to providers of:

- cloud hosting;
- databases;
- analytics;
- mapping;
- navigation;
- telecommunications;
- communications;
- customer support;
- identity verification;
- background verification;
- cybersecurity;
- document storage;
- AI services; and
- other technology required to operate Platform functions.

11.6 Insurance and Incident-Related Parties

Information may be disclosed to:

- insurers;
- insurance adjusters;
- workshops; and
- professional experts

where reasonably required to investigate an incident, vehicle claim or insurance matter.

11.7 Professional and Corporate Advisers

Information may be disclosed to:

- auditors;
- accountants;
- lawyers;
- corporate advisers;
- investors;
- lenders; and
- prospective transaction parties

under confidentiality and legal safeguards where appropriate.

11.8 Authorities

Information may be disclosed to:

- police;
- courts;
- regulators;
- tax authorities;
- licensing bodies;
- emergency services; and
- other government or legal authorities

when required or permitted by law, to protect rights or safety, or to investigate suspected unlawful activity.

11.9 Corporate Transactions

Information may be disclosed to affiliates, successors or acquiring entities in connection with:

- merger;
- acquisition;
- restructuring;
- financing; or
- transfer of all or part of Aider's business,

subject to applicable legal requirements.

Aider does **not sell or rent personal data for monetary consideration**.

If a future data practice would constitute “sale” or “sharing” under an applicable law, Aider will provide the disclosures and choices required by that law before implementing the practice.

12. THIRD-PARTY SERVICES, SDKs AND INDEPENDENT PROVIDERS

The Platform may depend on third-party:

- payment providers;
- mapping providers;
- cloud providers;
- telecommunications providers;
- analytics providers;
- customer-support providers;
- identity-verification providers;
- insurance providers; and
- other technology or service providers.

Third-party SDKs or integrations can process device or user data.

Aider is responsible for maintaining an accurate understanding of such integrations and for aligning app-store disclosures and this Policy with actual data practices.

Where a third party processes personal data on Aider's behalf, Aider will use reasonable contractual, security and oversight measures appropriate to the risk.

Where a third party independently determines its own purposes, its own privacy terms may also apply.

Links to external websites or services do not mean Aider controls their privacy practices.

13. CROSS-BORDER TRANSFERS AND PROCESSING

Because Aider operates or supports services in **Malaysia and Singapore** and may use regional or global service providers, personal data may be stored, accessed or processed outside the country where it was collected.

Aider will make cross-border transfers only where permitted by applicable law and will take reasonable steps to ensure the recipient provides a level of protection required by law, including through:

- contracts;
- due diligence;
- security controls;
- recognised transfer mechanisms; or
- other lawful safeguards as appropriate.

Where a cross-border booking or corporate/partner arrangement requires information to be available in another jurisdiction, Aider will limit the transferred information to what is reasonably necessary for the:

- service;
- safety;
- payment;
- support; or
- legal purpose involved.

14. DATA RETENTION, ARCHIVAL, LEGAL HOLDS AND DELETION

Aider retains personal data only for as long as reasonably necessary for the purposes described in this Policy, for the period required by applicable law, or while a valid legal, safety, fraud, accounting, audit, insurance, dispute or enforcement reason exists.

Retention periods differ by record type and risk.

Aider maintains or may maintain internal retention schedules that are more granular than this public Policy.

14.1 Account, Profile and Verification Records

Generally retained for the duration of the account or Platform relationship and thereafter only as reasonably needed for lawful purposes.

Retention may be extended for:

- legal or regulatory obligations;
- identity or fraud prevention;
- unresolved complaints;
- unresolved claims;
- enforcement;
- audit; or
- legal hold.

14.2 Booking, Trip, GPS and Operational Logs

Generally retained for:

- service fulfilment;
- safety;
- verification;
- analytics; and
- a risk-based period following service completion.

Retention may be extended for:

- disputes;
- chargebacks;
- incidents;
- insurance matters;
- suspected abuse;
- suspected fraud;
- investigations; or
- litigation.

14.3 Payments, Payouts, Invoices and Accounting

Generally retained for transaction processing and for periods required under applicable:

- tax;
- accounting;
- corporate; and
- financial-record obligations.

Retention may be extended for:

- audits;
- chargebacks;
- claims;
- regulatory requests; or
- litigation.

14.4 Communications, Support and Complaints

Generally retained for:

- customer service;
- quality;
- evidence; and
- a reasonable operational period.

Content hidden from the user interface may remain in restricted records where retention is justified.

Retention may be extended for:

- open cases;
- safety incidents;
- fraud;
- legal claims;
- regulatory requests; or
- law-enforcement requests.

14.5 Vehicle and Incident Photos and Reports

Generally retained for:

- condition verification;
- safety;
- service evidence; and
- claims handling.

Retention may be extended for:

- vehicle-damage claims;
- accident investigation;
- insurance investigation;
- legal holds; or
- enforcement.

14.6 Marketing and Preferences

Generally retained until:

- opt-out;
- consent withdrawal; or
- the relevant campaign purpose ends.

Aider may maintain minimal suppression records necessary to respect an opt-out.

Records may also be retained where necessary to demonstrate consent or withdrawal where required by law.

14.7 Security and Access Logs

Generally retained for a risk-based period appropriate to:

- cybersecurity;
- fraud detection; and
- incident investigation.

Retention may be extended for:

- security incidents;
- investigations;
- abuse prevention; or
- legal hold.

14.8 Backups

Data contained in backups may remain until it is overwritten or expires under Aider's backup rotation and disaster-recovery procedures.

Where technically required for recovery or subject to legal hold, backup information may be retained for longer.

Restored information remains subject to applicable deletion controls.

When retention is no longer justified, Aider will take reasonable steps to:

- delete;
- destroy;
- de-identify; or
- anonymise

the information.

De-identified or aggregated information that can no longer reasonably identify an individual may be retained for analytics, planning, security or statistical purposes.

15. ACCOUNT DELETION AND DATA DELETION REQUESTS

Where the Platform permits account creation, Aider will provide a reasonably accessible method to request account deletion, including:

- an in-app route where required by the relevant app store; and
- a web-based deletion route where required.

A deletion request is not treated merely as temporary account suspension.

After verifying the request and resolving necessary account or security checks, Aider will delete or de-identify personal data associated with the account unless retention is required or permitted for legitimate reasons including:

- legal or regulatory obligations;
- payment records;
- accounting records;
- fraud prevention;
- abuse prevention;
- open disputes;
- safety incidents;
- insurance claims;
- chargebacks;
- litigation; or
- legal holds.

Any retained data will be restricted to the relevant purpose and retained only for the necessary period.

Aider will also take reasonable steps to instruct service providers processing information on Aider's behalf to delete relevant information, subject to lawful retention and technical backup cycles.

Deletion may not immediately remove data from encrypted backups.

Deleted data should not be restored to active use except where required for disaster recovery and will remain subject to deletion controls.

16. YOUR RIGHTS AND CHOICES

Subject to applicable law, identity verification, exemptions and technical feasibility, you may have the right to:

- request access to personal data Aider holds about you;
- request information concerning certain uses or disclosures;
- request correction of inaccurate personal information;
- request updating of incomplete personal information;
- withdraw consent to processing that relies on consent, with reasonable notice and subject to consequences explained to you;
- request deletion of your account and associated information, subject to lawful retention;
- limit or object to certain processing where applicable;
- opt out of direct marketing;
- manage promotional communications;
- request portability or transmission of personal data where applicable law grants that right and the request is technically feasible and compatible;
- complain to Aider;
- complain to the relevant data-protection authority where applicable; and
- request human review or further information regarding certain significant automated decisions where applicable law provides such rights.

Aider may require sufficient information to verify identity and authority before acting on a request.

Where allowed by law, Aider may:

- refuse a request;
- limit a request;
- charge a permitted fee;
- redact third-party information; or
- request clarification.

Aider will respond within the time required by applicable law.

17. MARKETING AND PROMOTIONAL COMMUNICATIONS

Aider may send:

- marketing;
- promotions;
- rewards;
- referral offers; or
- service recommendations

through channels you have permitted, subject to applicable consent and direct-marketing rules.

You may opt out using:

- the unsubscribe mechanism;
- the stop mechanism;
- applicable app settings; or
- Aider's contact channels.

Opting out of marketing does not stop essential:

- booking communications;
- transaction communications;
- account communications;
- security communications;
- safety communications; or
- legal communications.

Aider may maintain a minimal suppression record, such as your contact identifier and opt-out status, to ensure your opt-out is respected.

Promotions may be analysed for:

- fraud;
- duplicate accounts;
- self-referrals;
- artificial booking activity; or
- other promotional abuse

in accordance with Platform rules.

18. APP PERMISSIONS AND DEVICE CONTROLS

18.1 Location

Aider may request approximate or precise location, in the foreground and, where justified, background.

Typical uses include:

- pickup and drop-off;
- nearby matching;
- dispatch;
- navigation;
- ETA;
- trip safety;
- route verification;
- arrival verification; and
- fraud or dispute evidence.

Location access will be requested through device permissions and, where required, a prominent in-app disclosure.

Certain functions may not work without location.

18.2 Camera, Photos and Gallery

Typical uses include:

- profile photographs;
- identity documents;
- driver verification;
- vehicle-condition photographs;
- incident evidence; and
- support attachments.

Permission is requested when the relevant feature is used.

Gallery access should be limited to selected content where technically available.

18.3 Microphone and Voice Communication

Typical uses include:

- optional in-app voice functions;

- calling functions; and
- other expressly disclosed audio features.

Microphone permission is requested only when needed.

Aider will provide additional notice if audio is recorded.

18.4 Notifications

Notifications may be used for:

- booking updates;
- driver arrival;
- customer arrival;
- safety alerts;
- account messages;
- security messages; and
- service communications.

These can generally be managed through app and device notification settings, subject to essential service and security messages.

18.5 Contacts

Contacts are not required for Aider's core service unless a specific:

- contact-selection;
- referral; or
- sharing feature

is offered.

Where offered, Aider should use selected-contact access or an equivalent privacy-preserving method rather than broad address-book access where reasonably available.

Operating-system permissions can normally be changed in device settings.

Revoking a permission may prevent the related feature from functioning.

Permission prompts are separate from acceptance of Platform Terms and separate from any consent required for a specific data-processing purpose.

19. COOKIES, ANALYTICS AND SIMILAR TECHNOLOGIES

Aider websites or web-based portals may use:

- cookies;
- local storage;
- pixels;
- SDKs; and
- similar technologies

for:

- authentication;
- security;
- preferences;
- functionality;
- analytics; and
- where permitted, marketing measurement.

Where consent is legally required for non-essential technologies, Aider will provide an appropriate consent or preference mechanism.

Aider will update disclosures if materially different tracking technologies are introduced.

20. SECURITY AND DATA PROTECTION BY DESIGN

Aider uses reasonable administrative, technical and organisational measures appropriate to the nature and risk of the information.

These measures may include:

- encrypted data transmission;
- role-based access;
- least-privilege access;
- authentication controls;
- logging;
- monitoring;
- secure hosting configurations;
- vendor due diligence;
- backup and recovery controls;
- incident-response procedures;
- staff confidentiality obligations; and

- restricted access to sensitive investigation records.

No technology or transmission method is completely secure.

Aider cannot guarantee absolute security, but will review controls and take reasonable corrective action when material risks are identified.

For higher-risk new features, Aider may conduct privacy or security impact assessments and apply data-protection-by-design principles appropriate to the feature and applicable regulatory guidance.

21. PERSONAL DATA BREACHES

If Aider becomes aware of a personal-data breach, Aider will:

- investigate the incident;
- contain the incident;
- assess its impact;
- notify the relevant authority where notification is legally required; and
- notify affected individuals where notification is legally required.

Notification timing, content and thresholds may differ by jurisdiction.

Aider may also implement measures such as:

- credential resets;
- account restrictions;
- forensic review; or
- enhanced monitoring

to reduce harm.

22. CHILDREN AND MINIMUM AGE

The consumer and driver Platform is intended for persons aged **18 and above** unless a specific service is expressly designed and lawfully configured for a younger person through:

- a parent;
- guardian;
- school;
- corporate client; or
- other authorised arrangement.

Aider does not knowingly permit minors to register as drivers.

If Aider discovers that personal data of a child has been collected without a valid basis or appropriate authorisation, Aider will take reasonable steps to delete or otherwise lawfully handle it.

23. DATA ABOUT OTHER PEOPLE

Bookings, corporate accounts, incident reports, trip-sharing, emergency assistance, vehicle records or partner programmes may involve personal data about other people.

You should only provide another person's personal data where:

- it is necessary; and
- you are authorised or otherwise permitted by law to provide it.

Aider may contact that person or request evidence of authority where needed to protect privacy, safety or account integrity.

24. CHANGES TO THIS POLICY

Aider may update this Policy when:

- services change;
- technology changes;
- data practices change;
- laws change;
- app-store rules change; or
- regulatory guidance changes.

The “**Last Updated**” date will be revised accordingly.

For material changes, Aider will provide notice through:

- the Platform;
- website;
- email;
- push notification; or
- another reasonable method

before or when the change becomes effective, as required by law.

Where new consent is legally required, continued use alone will not substitute for obtaining that consent.

25. MALAYSIA PRIVACY NOTICE

For processing governed by Malaysia’s **Personal Data Protection Act 2010 (Act 709)**, as amended, Aider intends this Policy to operate as part of its written Personal Data Protection Notice.

The notice identifies:

- the personal data processed;
- purposes of processing;
- sources of information;
- rights and choices;
- disclosure categories;
- security approach;
- retention approach; and
- contact channels.

Aider will make the notice available in **Bahasa Malaysia and English** and will obtain consent separately where required.

Malaysia data subjects may exercise rights available under Act 709, including:

- access;
- correction;
- withdrawal or limitation rights where applicable; and
- data portability subject to statutory conditions, technical feasibility and compatibility.

Aider will comply with applicable requirements concerning:

- data processors;
- security;
- cross-border transfer;
- Data Protection Officer appointment; and
- personal-data-breach notification.

26. SINGAPORE PRIVACY NOTICE

Where Singapore's **Personal Data Protection Act 2012** applies, Aider will process personal data in accordance with applicable obligations including:

- accountability;
- notification;
- consent;
- purpose limitation;
- accuracy;
- protection;
- retention limitation;
- transfer limitation;
- access and correction; and
- data-breach notification requirements.

Aider will designate the required data-protection contact or DPO and make the relevant business contact information publicly available.

If a corporate or partner arrangement in Singapore allocates particular processing responsibilities differently, the relevant contract or data-processing terms may supplement this Policy without reducing individuals' rights under applicable law.

27. CONTACT, PRIVACY REQUESTS AND COMPLAINTS

For privacy questions, access, correction, deletion, portability requests, consent withdrawal or complaints, contact Aider through the following official channels:

Company:

MYAIDER HOLDING SDN. BHD.

Company Registration No. 202301007378

Attention:

Data Protection / Privacy

Email:

customerservice@myaider.com

Phone:

+60 17-711 6865

Address:

Southgate Commercial Center

D-06-15, Jalan Dua

Chan Sow Lin

55200 Kuala Lumpur, WPKL

Malaysia

Official Website:

www.myaider.com

Aider may publish a dedicated DPO or privacy business contact on the official website or Platform.

Where a dedicated DPO contact is published, that contact should be used for formal data-protection correspondence.

Operational Requirement Before Publication

Aider should ensure that the privacy contact is actively monitored and, where DPO appointment is required, publish the designated DPO's business contact details and register or notify the appointment as required by the applicable regulator.

28. LANGUAGE AND INTERPRETATION

This Policy is intended to be available in **English and Bahasa Malaysia**.

Both versions are intended to communicate the same privacy practices.

If a discrepancy arises, Aider will interpret and apply the Policy in a manner that complies with the mandatory requirements of the applicable data-protection law.

Nothing in this Policy limits any non-waivable right of a data subject or obligation of Aider under applicable law.

END OF PRIVACY POLICY

© 2026 MYAIDER HOLDING SDN. BHD.
All Rights Reserved.