Data Processing Agreement

Smart Lead & Ticket Routing for Workflows - UK Company

Daeda Technologies Ltd - Company No. 17360943 - England and Wales

This Data Processing Agreement (the "DPA") is entered into as of the Effective Date by and between the customer identified below ("Customer") and Daeda Technologies Ltd ("Daeda"). It applies to every free, trial, or paid tier of the Services identified below unless the parties expressly agree otherwise in writing.

Completion Fields

Effective Date	
Customer legal name	
Customer address	
Customer privacy contact	
Main Agreement	Daeda Workflow Apps SaaS Terms
Services	Smart Lead & Ticket Routing for Workflows

1. Status and relationship to the Main Agreement

1.1 This DPA forms part of the Main Agreement governing Customer's use of the Services. If Customer uses a free or trial tier without a separately signed Main Agreement, the online terms accepted for the Services are the Main Agreement.

1.2 If this DPA conflicts with the Main Agreement in relation to the processing of Customer Personal Data, this DPA controls. Liability, indemnity, warranty, payment, and other commercial provisions remain governed by the Main Agreement unless this DPA expressly states otherwise.

1.3 The Schedules form part of this DPA. References to legislation include amendments and replacement legislation applicable to the relevant processing.

1.4 Under a written business-transfer and assignment agreement, this DPA and the related Main Agreement automatically transfer from Daeda Technologies Pte. Ltd. to Daeda Technologies Ltd with effect from 6 September 2026 to the extent that the original agreement and Applicable Data Protection Law permit assignment or transfer without further Customer consent. From that date, Daeda Technologies Ltd assumes the processor or subprocessor role under each transferred agreement. This Section does not override a signed or negotiated agreement that prohibits transfer, requires consent or novation, identifies another contracting entity, or specifies a different effective date. Where such a requirement applies, the affected agreement remains with Daeda Technologies Pte. Ltd. until the requirement is satisfied.

2. Definitions

2.1 "Applicable Data Protection Law" means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 where applicable, the EU GDPR where it applies to the processing, and other binding data protection law applicable to the parties' processing under the Services.

2.2 "Customer Personal Data" means Personal Data processed by Daeda on behalf of Customer in providing the Services. It excludes Personal Data for which Daeda acts as an independent controller as described in Section 13.

2.3 "EU GDPR" means Regulation (EU) 2016/679. "UK GDPR" has the meaning given in section 3(10) of the Data Protection Act 2018.

2.4 "Personal Data", "Personal Data Breach", "processing", "controller", "processor", and "data subject" have the meanings given by Applicable Data Protection Law.

2.5 "Restricted Transfer" means a transfer of Personal Data requiring an adequacy regulation, adequacy decision, appropriate safeguard, exception, or other transfer mechanism under Applicable Data Protection Law.

2.6 "Subprocessor" means a processor engaged by Daeda to process Customer Personal Data on Customer's behalf. A platform or provider selected and contracted by Customer is not a Daeda Subprocessor solely because Customer instructs Daeda to interoperate with it.

3. Roles, scope, and Customer instructions

3.1 Customer is controller and Daeda is processor of Customer Personal Data. If Customer acts as a processor for another controller, Daeda acts as Customer's subprocessor and Customer warrants that its instructions and appointment of Daeda are authorised by the relevant controller.

3.2 Daeda will process Customer Personal Data only on Customer's documented instructions, including the Main Agreement, this DPA, Customer's configuration and use of the Services, and other written instructions accepted by Daeda. Daeda will not sell Customer Personal Data.

3.3 Daeda will immediately inform Customer if, in Daeda's reasonable opinion, an instruction infringes Applicable Data Protection Law. Daeda may suspend the affected processing while the parties resolve the issue.

3.4 If law requires Daeda to process Customer Personal Data other than on Customer's instructions, Daeda will notify Customer before processing unless that law prohibits notice on important grounds of public interest.

3.5 The subject matter, duration, nature and purpose of processing, categories of Personal Data, categories of data subjects, and Customer's rights and obligations are described in this DPA and Schedule 2.

4. Customer obligations

4.1 Customer will:

- comply with Applicable Data Protection Law and provide all required notices;
- have a valid lawful basis for the processing and for providing Customer Personal Data to Daeda;
- give lawful, fair, and documented instructions;
- configure permissions, data scope, users, integrations, and retention appropriately;
- limit Customer Personal Data to what is reasonably necessary for the Services; and
- ensure its credentials, authorised users, and connected systems are appropriately secured.

4.2 Customer must not intentionally use the Services for children's data, criminal-offence data, government identification data, payment-card data, health records, or other specially protected data unless the processing is lawful, necessary, supported by appropriate safeguards, and expressly agreed where additional safeguards are required.

5. Confidentiality and personnel

5.1 Daeda will ensure that persons authorised to process Customer Personal Data are subject to a binding duty of confidentiality and process it only as necessary to perform their duties.

5.2 Daeda will limit access to authorised personnel with a need to operate, support, secure, or maintain the Services and will provide appropriate data protection and security awareness.

5.3 Daeda personnel are ordinarily based in the United Kingdom. Authorised personnel may access the Services while temporarily travelling, including within Europe, subject to Daeda's access-control, device-security, and confidentiality requirements.

6. Security

6.1 Taking into account the state of the art, implementation costs, and the nature, scope, context and purposes of processing, as well as the risk to individuals, Daeda will implement and maintain appropriate technical and organisational measures designed to protect Customer Personal Data.

6.2 The current measures are described in Schedule 3. Daeda may update them as technology and the Services evolve, provided the update does not materially reduce the overall protection of Customer Personal Data.

6.3 Customer acknowledges that no service can guarantee absolute security and that Customer is responsible for securely configuring its own HubSpot account, AI client, user devices, credentials, permissions, and connected providers.

7. Subprocessors

7.1 Customer grants Daeda general written authorisation to engage the Subprocessors listed in Schedule 4.

7.2 Before a Subprocessor processes Customer Personal Data, Daeda will impose written data protection obligations that provide a level of protection substantially equivalent to the obligations applicable to Daeda under this DPA, to the extent required by Applicable Data Protection Law. Daeda remains responsible for its Subprocessors' performance of those obligations.

7.3 Daeda will give Customer at least 30 days advance notice before adding or replacing a Subprocessor that materially processes Customer Personal Data, unless an emergency replacement is reasonably required to protect security, availability, or legal compliance.

7.4 Customer may object during the notice period on reasonable data protection grounds. The parties will work in good faith to resolve the objection. If they cannot do so, Customer may stop using or terminate the affected Services in accordance with the Main Agreement.

7.5 HubSpot and customer-selected AI providers are separately identified in Schedule 4 because their roles depend on the Customer's direct relationships and instructions.

8. Data subject requests

8.1 Taking into account the nature of the processing, Daeda will provide reasonable assistance through appropriate technical and organisational measures to help Customer respond to requests to exercise data subject rights.

8.2 If Daeda receives a request relating to Customer Personal Data, Daeda will refer it to Customer and will not respond substantively except on Customer's documented instructions or as required by law.

8.3 Customer remains responsible for verifying the requester's identity, deciding the response, and responding within applicable time limits. Customer is also responsible for data that remains in Customer's HubSpot account or customer-selected providers.

9. Compliance assistance

9.1 Taking into account the nature of processing and information available to Daeda, Daeda will reasonably assist Customer with:

- security obligations;
- Personal Data Breach notifications and communications;
- data protection impact assessments; and
- prior consultation with a supervisory authority where required.

9.2 Assistance beyond the ordinary operation of the Services may be subject to reasonable fees where permitted by the Main Agreement, unless the assistance is required because Daeda breached this DPA.

10. Personal Data Breaches

10.1 Daeda will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data.

10.2 The notification will include available information reasonably required for Customer to meet its legal obligations, including the nature of the breach, likely consequences, affected data and individuals, and measures taken or proposed. Daeda may provide information in phases as it becomes available.

10.3 Notification is not an admission of fault or liability. Daeda will take reasonable steps to contain, investigate, mitigate, and remediate the breach.

11. Information and audits

11.1 Daeda will make available information reasonably necessary to demonstrate compliance with this DPA and Article 28 of the UK GDPR or EU GDPR, as applicable.

11.2 Daeda may satisfy routine review requests using written responses, policies, security documentation, Subprocessor information, and similar evidence.

11.3 Audits and inspections are limited to once in any 12-month period, except following a material Personal Data Breach, a request from a competent supervisory authority, or reasonable evidence of material non-compliance. They require reasonable advance notice, must occur during normal business hours, must be subject to confidentiality, and must minimise disruption and risk to the Services and other customers.

11.4 An audit may not access other customers' data, source code, credentials, security secrets, or live production systems unless legally required and no less intrusive evidence can reasonably satisfy the requirement.

11.5 Customer bears reasonable audit costs unless the audit identifies material non-compliance by Daeda.

12. Return and deletion

12.1 At the end of the Services, Daeda will, at Customer's choice, delete or return Customer Personal Data and delete remaining copies, unless applicable law requires continued storage. Customer must communicate its choice in writing within a reasonable period.

12.2 Until deletion or return is completed, Daeda will continue to protect Customer Personal Data under this DPA.

12.3 Schedule 2 describes current product-specific retention and deletion behaviour. It does not create a retention promise for systems or data categories not expressly listed.

12.4 Daeda may preserve limited information where required by law or reasonably necessary for security, fraud prevention, accounting, taxation, dispute resolution, or legal claims. Such information will remain protected and will not be used for an incompatible purpose.

12.5 Customer remains responsible for deleting or modifying data held in Customer's HubSpot account, AI provider, AI client, or other customer-controlled systems.

13. Daeda as an independent controller

13.1 Daeda may act as an independent controller for business contact details, contract administration, billing and taxation records, fraud and abuse prevention, legal compliance, and the establishment, exercise, or defence of legal claims.

13.2 Processing in that independent-controller capacity is governed by Daeda's applicable privacy notice and is outside Customer's processor instructions under this DPA.

14. International transfers

14.1 Daeda will make a Restricted Transfer only on Customer's documented instructions and using a lawful transfer mechanism where required.

14.2 Transfers from the EEA to Daeda in the United Kingdom may rely on the European Commission's applicable adequacy decision for the United Kingdom while it remains in force. Transfers from the United Kingdom to the EEA may rely on applicable UK adequacy regulations.

14.3 Where adequacy does not apply, the parties will use the applicable EU Standard Contractual Clauses, UK International Data Transfer Agreement, UK Addendum, or another lawful safeguard. Schedule 5 provides conditional transfer terms.

14.4 Daeda will use reasonable measures to limit third-country access to what is necessary for the Services and to protect Customer Personal Data during transfer.

15. Term and legal effect

15.1 This DPA begins on the Effective Date and continues while Daeda processes Customer Personal Data on Customer's behalf.

15.2 Sections intended to protect Customer Personal Data after termination survive for as long as Daeda retains that data.

15.3 If any provision is invalid or unenforceable, it will be modified to the minimum extent necessary, and the remaining provisions will continue in effect.

16. Governing law and jurisdiction

16.1 Except where mandatory Applicable Data Protection Law or incorporated transfer clauses require otherwise, this DPA is governed by England and Wales and the parties submit to the courts of England and Wales.

17. Signatures

By signing below, each party confirms that it has authority to enter into this DPA and agrees that the Schedules form part of it.

Daeda Technologies Ltd
Role: Processor

_____
Signature

Jack Tolley — Director

Name — Title

Date

Customer identified in the Completion Fields
Role: Controller

_____
Signature

Name — Title

Date

Schedule 1 - Parties

Customer / Controller

Name: Customer identified in the Completion Fields
Address: See Completion Fields
Privacy contact: See Completion Fields
Activities relevant to the processing: Customer determines the purposes and means of processing Customer Personal Data through its HubSpot account, product configuration, authorised users, connected systems, and documented instructions.
Signature and date: See the signature page.

Daeda / Processor

Name: Daeda Technologies Ltd
Company number: 17360943
Registered office: 167-169 Great Portland Street, Fifth Floor, London, England, W1W 5PF
Privacy contact: contact@daeda.tech
Activities relevant to the processing: Provision of Smart Lead & Ticket Routing for Workflows as described in this DPA and Schedule 2.
Signature and date: See the signature page.

Schedule 2 - Smart Routing Processing Details

1. Subject matter

Provision, maintenance, security, support, internal usage measurement, billing, and administration of Smart Lead & Ticket Routing for Workflows, a HubSpot Marketplace workflow application providing lead, ticket, and CRM record routing, round-robin assignment, owner-property updates, and out-of-office workflow actions.
The current production backend is https://workflow-ooo.daeda.tech and the HubSpot Marketplace application is named "Smart Lead & Ticket Routing for Workflows".

2. Duration

Processing continues for the term of Customer's use of the Services and for the period necessary to complete the return or deletion process, resolve security or billing matters, and comply with applicable legal obligations.
No fixed rolling retention period is promised for account records, routing state, logs, analytics, support correspondence, credentials, backups, or billing records unless expressly agreed in writing.

3. Categories of data subjects

- Customer's HubSpot users, owners, sales representatives, service representatives, administrators, team managers, employees, and contractors.
- Leads, contacts, customers, prospects, ticket requesters, company representatives, deal participants, quote participants, and other CRM or workflow participants whose records enter Customer-configured workflows.
- Customer personnel who install, administer, use, receive support for, or are billed for the Services.

4. Categories of Customer Personal Data

- Account and installation information: HubSpot portal ID, installation email, install/uninstall state, plan tier, usage counts, Stripe customer ID, OAuth tokens, token expiry, granted scopes, and related authentication metadata.
- HubSpot user and owner information: name, email address, user ID, owner ID, team IDs, team membership, accessible or shared teams, deactivation status, and administrator or team-manager status.
- Availability and out-of-office information: availability, in-working-hours and out-of-office status, event dates and times, event titles or reasons where configured by Customer, and event identifiers.
- Workflow and routing configuration: workflow ID, action ID, selection mode, selected users or teams, rotation order, last assigned user, timestamps, fallback behaviour, watched availability properties and operators, and owner-property names.
- CRM and workflow metadata: object type, object ID, selected property names, assigned owner ID, assigned user name, skipped-user count, and action outputs.
- Customer-authorised objects and property metadata where optional scopes are enabled, including contacts, companies, deals, tickets, quotes, leads, custom objects, invoices, orders, and commerce payments.
- Support, security, telemetry, and operational information: request metadata, event names, portal or user identifiers, application metadata, UUIDs, settings properties, sanitised error information, operational alerts, and support communications.

5. Sensitive data

The Services are not designed to require special-category data, criminal-offence data, payment-card data, government-identification data, medical data, or children's data.

Availability and out-of-office fields may reveal sensitive circumstances if Customer enters health, religious, trade-union, or similar details in titles, reasons, descriptions, labels, or support messages. Customer is responsible for avoiding such details unless their processing is lawful and necessary.

6. Nature of processing

Daeda may receive, retrieve, host, store, cache, log, inspect, transform, validate, compare, route, assign, update, transmit, return, and delete Customer Personal Data as needed to provide the Services.

Current processing includes:

- authenticating HubSpot requests and maintaining OAuth-backed HubSpot API access;
- reading HubSpot users, teams, account timezone, workflow metadata, availability fields, out-of-office hours, and owner-compatible properties;
- selecting an available user according to Customer's round-robin configuration;
- storing account, routing, rotation, administrator, team, usage, and billing-related state;
- optionally updating owner-compatible properties where Customer grants the required scope;
- adding, clearing, and reading HubSpot out-of-office events or hours;
- enforcing plan limits, creating billing links, and recording usage;
- recording limited internal usage and operational metrics; and
- sending limited structured operational alerts for installations, account and billing lifecycle events, scope failures, and application incidents.

7. Purposes

- Provide, operate, maintain, secure, monitor, and support the Services.
- Execute Customer-configured HubSpot workflow actions.
- Route CRM records to Customer-selected users and teams.
- Maintain rotation state and avoid users marked unavailable.
- Process configured out-of-office and availability actions.
- Administer installation, authentication, permissions, billing, plan limits, and support.
- Detect, investigate, and resolve errors, abuse, security incidents, and operational issues.
- Comply with law and enforce the Main Agreement.

8. Customer rights and obligations

Customer determines the workflows, users, teams, properties, fallbacks, optional scopes, and records processed by the Services. Customer may change its configuration, uninstall the application, request assistance with data subject rights, and exercise the deletion or return choice described in Section 12 of the DPA.

Customer remains responsible for data held in its HubSpot account and for configuring workflows and fields lawfully.

9. Retention and deletion

Customer Personal Data is retained for the duration described in Section 2 and then returned or deleted in accordance with Section 12 of the DPA. No more specific product retention interval is represented in this Schedule.

Schedule 3 - Technical and Organisational Measures

Daeda does not claim SOC 2, ISO 27001, or another formal security certification in this DPA. The measures below describe current controls and will be reviewed as the Services evolve.

1. Access control and confidentiality

- Production access is limited to authorised personnel with a need to operate, support, secure, or maintain the Services.
- Authorised personnel are subject to confidentiality obligations.
- Multi-factor authentication is used where supported by the relevant production service.
- Password-manager tooling is used for production credentials.
- Administrative devices use encrypted storage where supported by the operating system and device.
- Least-privilege access is applied in light of Daeda's small-team operating model.

2. Authentication and credential handling

- HubSpot access uses OAuth and scopes granted by Customer.
- Production secrets are supplied through environment or secret-management mechanisms rather than hard-coded into source.
- HubSpot OAuth access and refresh tokens are stored using application-level AES-256-GCM envelope encryption in the current account storage implementation.
- License and service credentials are treated as confidential and can be revoked through available product or administrative controls.

3. Transmission and network security

- Customer-facing production endpoints and HubSpot API calls use HTTPS/TLS.
- Services are containerised and operated behind Kubernetes service and ingress infrastructure.
- Network access and permitted customer-facing URLs are limited by application and platform configuration.

4. Storage, segregation, and minimisation

- Persistent account, configuration, usage, and product records are stored in Supabase.
- Customer records and operational state are logically separated using HubSpot portal identifiers and product-specific mappings.
- Daeda limits collection to product configuration, selected records and properties, operational metadata, and other information needed to provide the Services.
- Daeda does not intentionally create routine bulk local support exports. Local files, screenshots, or support dumps should be limited to approved support, security, legal, or incident-response needs.

5. Availability, logging, and incident response

- The Services use containerised application components and persistent product storage.
- Operational logs and available product records are used to investigate errors, security events, and suspected Personal Data Breaches.
- Daeda maintains procedures to contain, investigate, mitigate, and communicate material security incidents.
- This DPA does not promise a fixed backup, recovery-time, log-retention, or availability service level unless separately agreed in writing.

6. Data subject and deletion support

- Daeda uses available records and product controls to assist Customer with access, correction, restriction, export, or deletion requests.
- Customer remains responsible for data retained in HubSpot and other customer-controlled providers.
- Product-specific deletion controls are described in Schedule 2.

7. Product-specific controls

- Workflow requests are authenticated using HubSpot request and portal context.
- Optional direct owner-property updates require additional Customer-granted HubSpot scopes.
- Routing state is limited primarily to portal, workflow, action, user, team, selection, and last-assignment information rather than full copies of CRM records.
- A short-lived in-memory cache is used for selected HubSpot user lookups.
- External operational alerts are restricted to non-customer metadata such as the application, event type, timestamp, generic environment, and a random incident identifier. Customer Personal Data and customer-linked identifiers are excluded.
- External product-analytics event delivery is disabled. Schedule 4 must be updated before an external analytics processor is used for Customer Personal Data.

Schedule 4 - Smart Routing Subprocessors and Connected Platforms

Customer generally authorises the following providers for the processing described below. Locations describe Daeda's current configuration as at 22 August 2026.

Provider	Role	Processing and location
Supabase	Database and backend platform	Account and installation metadata, encrypted OAuth token fields, routing and assignment state, administrator/team mappings, usage, billing metadata, and operational records. Current project region recorded as EU Central 1, Frankfurt, Germany.
Hetzner	Application hosting	Container, Kubernetes ingress, networking, and infrastructure used to operate https://workflow-ooo.daeda.tech. Current location recorded as Falkenstein, Germany.
Stripe	Billing platform	Paid checkout, customer portal, subscription, Stripe customer identifiers, and billing events. Stripe may process data globally under its applicable terms and transfer safeguards.
HubSpot	Customer-connected CRM and workflow platform	Customer's HubSpot account, APIs, users, teams, workflows, CRM records, owner properties, and OAuth authorisation. HubSpot may be Customer's independent provider where Customer has a direct HubSpot agreement and instructs Daeda to use its APIs.

Transfer notes

- Supabase and Hetzner are currently recorded as EEA infrastructure locations.
- Stripe and HubSpot may process information outside the UK or EEA subject to their applicable terms, locations, and transfer safeguards.
- Daeda personnel are ordinarily based in the United Kingdom and may access the Services temporarily while travelling under Schedule 3 controls.

Schedule 5 - Conditional International Transfer Terms

This Schedule applies only to a Restricted Transfer not already covered by an applicable adequacy regulation or adequacy decision. It does not convert temporary access by an authorised employee of Daeda Technologies Ltd while travelling into a separate recipient or Subprocessor relationship.

1. Current location position

- Daeda is established in the United Kingdom and its personnel are ordinarily based there.
- Authorised Daeda personnel may access the Services temporarily while travelling, including within Europe, subject to Daeda's security and confidentiality controls.
- Current product infrastructure and vendor locations are described in Schedule 4 and on Daeda's public Subprocessor List.
- An EEA Customer may rely on the applicable European Commission adequacy decision for transfers to the United Kingdom while that decision remains in force.

2. EU Restricted Transfers

Where an EU Restricted Transfer from Customer to Daeda requires an Article 46 safeguard, the parties incorporate the European Commission Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor), as amended or replaced according to their terms (the "EU Transfer SCCs").

The following selections apply unless the parties record different lawful selections in writing:

- Clause 7 docking clause: applies.
- Clause 9 use of subprocessors: Option 2, general written authorisation.
- Subprocessor notice period: 30 days.
- Clause 11 optional redress language: not selected.
- Clause 17 governing law: an EU Member State law selected in the Completion Fields or, if none is selected, Ireland.
- Clause 18 courts: the courts corresponding to the Clause 17 governing law or, if none is selected, the courts of Ireland.
- Annex I parties and transfer description: Schedules 1, 2, and 4 of this DPA.
- Annex II technical and organisational measures: Schedule 3 of this DPA.
- Annex III subprocessors: Schedule 4 of this DPA.

The competent supervisory authority will be determined under Clause 13 of the EU Transfer SCCs based on the Customer's establishment, representative, and affected individuals.

3. UK Restricted Transfers

Where a UK Restricted Transfer from Customer to Daeda requires an Article 46 safeguard and the parties rely on the EU Transfer SCCs, the parties incorporate the then-current ICO-approved International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "UK Addendum") to the extent permitted by its mandatory terms.

For the UK Addendum:

- Customer is the exporter and Daeda Technologies Ltd is the importer.
- The selected SCCs are Module Two and the selections in Section 2 above.
- The appendix information is contained in Schedules 1 to 4 of this DPA.
- Neither party may end the UK Addendum solely because the approved form changes unless its mandatory terms, the Main Agreement, or Applicable Data Protection Law permits termination.
- The mandatory clauses of the approved UK Addendum prevail over conflicting terms of this DPA for the relevant UK Restricted Transfer.

The parties may instead execute the UK International Data Transfer Agreement or use another lawful safeguard.

4. Onward transfers

Daeda will not make an onward Restricted Transfer to a Subprocessor unless the transfer is covered by adequacy, applicable standard contractual clauses, an approved addendum, a recognised data privacy framework, or another lawful mechanism.

Where required, Daeda will carry out or reasonably assist with a proportionate transfer risk assessment, transfer impact assessment, or data protection test using information reasonably available about the recipient, location, data, safeguards, and practical risk.