

Data Processing Agreement (Version 3.1, August 2026)

■ 1. Introduction

This Data Processing Agreement ("**DPA**") forms part of, and is subject to, the agreement for Customer's use of the Services between Requesty Ltd (registered in England & Wales under company number 15165717) of 71-75 Shelton Street, Covent Garden, London WC2H 9JQ ("**Requesty**", "**we**", "**us**", "**our**") and the customer identified in the Order Form or online registration ("**Customer**", "**you**", "**your**"), individually a "**Party**" and together the "**Parties**".

This DPA sets out the terms on which Requesty will process Personal Data on behalf of Customer in connection with the services described in the Agreement (the "**Services**"). It replaces and supersedes all prior DPAs between the Parties as of the Effective Date.

Effective Date: the earlier of (i) Customer's first use of the Services, or (ii) the date of last signature by the Parties below. This DPA applies where incorporated by reference in an Order Form.

Nothing in this DPA relieves either Party of its direct responsibilities or liabilities under Data Protection Legislation.

1.1 The Agreement. "Agreement" means (i) the Requesty Terms of Service published at <https://requesty.ai/terms>, as accepted by Customer, together with any Order Form, or (ii) where the Parties have executed one, a Master Services Agreement. Where no separate written agreement has been executed, the Terms of Service are the Agreement for the purposes of this DPA, and references in this DPA to the Agreement, including for confidentiality, liability and governing law, are references to those Terms of Service.

1.2 Relationship to the Terms of Service. This DPA supplements and does not replace the commitments Requesty gives in the Terms of Service, including Section 5 (Model Terms), Section 6.2 (No Training / No Selling), Section 6.3 (Logging Options) and Section 6.6 (Data Breach Notification). Where this DPA and the Terms of Service conflict on a data protection matter, this DPA prevails.

1.3 Standard terms. This is Requesty's standard Data Processing Agreement. It applies to every Customer, takes effect on acceptance of the Agreement and does not require separate signature to be binding. Requesty publishes the current version at <https://requesty.ai/dpa>. Per key logging control under clause 5.2 and use of the EU Endpoint under clause 5.4(a) are available on all plans. Organisation wide Zero Data Retention under clause 5.3, strict server side endpoint enforcement under clause 5.4(a) and Approved Models under clause 5.5 are enabled by Requesty on request and may require the Enterprise plan. No provision of this DPA is conditional on Customer's level of spend. Requesty does not negotiate amendments to this DPA other than as part of a Master Services Agreement executed by Requesty. Acceptance of the Agreement constitutes acceptance of this DPA in the form published at that time.

■ 2. Definitions

Capitalised terms not defined herein have the meanings set out in the Agreement. The

following terms have the meanings set opposite them:

- **"Applicable Data Protection Legislation"** means all laws and regulations worldwide applicable to the Processing of Personal Data under the Agreement, including (where applicable) the UK GDPR, EU GDPR, Data Protection Act 2018, e-Privacy Regulations, and any legislation replacing or supplementing the foregoing.
- **"Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Process/Processing", "Processor", and "Supervisory Authority"** have the meanings given in the UK GDPR (and the EU GDPR where relevant).
- **"Large Language Model Routing Platform" (or "LLM Router")** means Requesty's cloud service that receives Customer prompts, routes them to third-party foundation-model providers selected by Customer or by Requesty acting on Customer's instructions, and returns the model response to Customer.
- **"Logging"** means the storage by the Services of prompts, model outputs, and related metadata in Requesty's databases for debugging, analytics, billing, or support.
- **"Model Provider"** means a third party provider of a foundation or large language model to which Requesty routes a request as a result of Customer's model selection or Customer's configuration of the Services.
- **"Infrastructure Sub-processor"** means a Sub-processor engaged by Requesty to operate the Services for all customers, including hosting, storage, logging, monitoring, payment and support tooling, as listed in Part A of the page referred to in clause 8.1.
- **"Approved Models"** means the list of models that Customer permits for its organisation in the Services, outside of which Requesty rejects requests.
- **"Training Permitted Model"** means a model that Requesty labels in the Services as one in respect of which the Model Provider retains prompts and outputs and may use them to train, fine tune or otherwise improve models, as described in clause 5.9.
- **"Free Plan"** means use of the Services under a plan for which Requesty charges no fees for the Services.
- **"Paid Plan"** means any other plan, including pay as you go, committed spend and Enterprise plans.
- **"EU Endpoint"** means <https://router.eu.requesty.ai>.
- **"Zero Data Retention" or "ZDR"** means the organisation level configuration described in clause 5.3.
- **"Trust Centre"** means Requesty's trust centre at <https://trust.requesty.ai>, where its current security documentation, certification status and sub-processor information are published.
- **"Standard Contractual Clauses" or "SCCs"** means the standard contractual clauses annexed to Commission Decision EU 2021/914 (Modules 1, 2 and 3) as incorporated by reference in Schedule 2, and as modified by the UK International Transfer Addendum where applicable.
- **"Account Information"** means business contact, billing, tax, fraud-prevention and support case data relating to Customer's personnel and representatives that Requesty processes outside of the LLM Router.
- **"Restricted Transfer"** means a transfer of Personal Data that is restricted under Chapter V of the EU GDPR and/or UK GDPR.
- **"US State Privacy Laws"** means state privacy laws in force in the United States,

including the CCPA/CPRA, VCDPA, CPA, CTDPA and UCPA.

■ 3. Roles of the Parties

3.1 The Parties acknowledge that, for the purposes of Data Protection Legislation, **Customer is the Controller** and **Requesty is the Processor** in respect of Personal Data Processed when providing the Services. Where Customer itself acts as a processor for an ultimate third-party controller, Requesty is Customer's **sub-processor**.

3.2 Each Party will comply with the obligations that apply to it under Applicable Data Protection Legislation. Customer warrants that its instructions to Requesty (as set out in this DPA and as may be otherwise documented in writing) are lawful.

3.3 For Account Information, the Parties acknowledge that Customer and Requesty act as **independent controllers**. Module 1 of the SCCs (and, where applicable, the UK Addendum) applies to any Restricted Transfer of Account Information.

■ 4. Description of Processing

The subject-matter, nature, purpose and duration of Processing, together with the categories of Personal Data and Data Subjects, are set out in **Schedule 1 (Processing Particulars)**.

■ 5. Customer Instructions & Logging Options

5.1 Requesty will Process Personal Data **only on documented instructions from Customer**, unless required to do so by applicable law. The Agreement, this DPA, and Customer's configuration of the Services (via UI, API, or support ticket) constitute Customer's complete and final instructions.

5.2

	Prompt/Response	Logging	Control.
Customer may, at any time:			

- **Enable Logging** (default): Requesty will store prompts, model outputs, and certain metadata (e.g. timestamps, model ID, latency) in encrypted form for the retention period stated in Schedule 1.
- **Disable Logging**: Requesty will not persist prompts or model outputs in its databases. Minimal metadata required for billing (e.g. token counts, model ID, timestamp) will be retained for the period stated in Schedule 1 (Logging Options and Retention), after which it is deleted or anonymised.

The selected option can be changed at any time and applies prospectively to subsequent requests. Customer is solely responsible for verifying that its chosen setting meets its compliance requirements.

5.3 Zero Data Retention. On Customer's written request Requesty will enable Zero Data Retention for the whole of Customer's organisation. Where ZDR is enabled: (a) prompts, model outputs, tool call content and attachments are processed in transit only and are not written to persistent storage by Requesty; (b) Requesty side prompt caching is disabled; (c) the setting is enforced by Requesty server side for the entire organisation and cannot be overridden by an individual API key, user, project or request parameter; (d) Requesty retains only the content free telemetry described in Schedule 1; and (e) Requesty confirms activation

to Customer in writing. ZDR remains in force until an authorised administrator of Customer requests its removal in writing. Zero Data Retention governs Requesty's own Processing only. It does not prevent a Model Provider from retaining prompts or outputs, or from using them to train or improve models. What happens at the Model Provider is determined by the model Customer selects, as described in clauses 5.7 and 5.9. Customer restricts Model Provider retention by restricting Approved Models under clause 5.5, not by enabling Zero Data Retention.

5.4 EU Data Residency. Customer Personal Data stored by Requesty is stored in Frankfurt, Germany (EEA) in all cases. Residency operates in two layers and Customer acknowledges that both are required for Processing to remain within the EEA end to end:

(a) Requesty layer. Where Customer uses the EU Endpoint, all Requesty side Processing, including request handling, routing, caching where enabled, Logging where enabled, analytics and storage, is performed exclusively in data centres located in the EEA. On Customer's written request Requesty will apply strict server side enforcement, under which any request made by Customer's organisation to a non EU endpoint is rejected rather than served, so that residency does not depend on client side configuration.

(b) Inference layer. Where the model inference itself is performed is determined by the model Customer selects, not by the endpoint Customer calls. Use of the EU Endpoint does not by itself relocate inference into the EEA. To keep inference within the EEA, Customer must restrict Approved Models to model deployments hosted in the EEA. Requesty publishes the hosting region of each model, and the Model Provider's published position on retention and on use of content for training, through the Services and at <https://requesty.ai/models>.

5.5 Approved Models. Where Customer configures Approved Models, Requesty rejects any request for a model outside that list, including on failover, load balancing and automatic routing, and will not substitute a different model, provider or hosting region. Fallback operates only within the Approved Models.

5.6 Caching. Requesty side prompt caching, where Customer enables it, stores cache entries within the EEA for the lifetime stated in the Documentation and is disabled where ZDR is enabled. Provider side prompt caching is a feature of the relevant Model Provider, is ephemeral, and is governed by that provider's published terms. Customer may disable caching at any time in the Services.

5.7 Model Providers. Customer selects the models it uses. For each model Requesty surfaces the Model Provider, the hosting region and the provider's published position on retention and on use of content for training. That metadata reproduces the Model Provider's own published policy. Requesty checks it against the provider's published terms and updates it when Requesty becomes aware of a change, and gives no warranty as to the accuracy of a third party's published statements or as to that provider's compliance with them. Requesty's obligations in respect of Model Providers are set out in clause 8. Where a Model Provider's published position is that it retains prompts and outputs and uses them to train or improve models, clause 5.9 applies.

5.8 Unlawful instructions. Requesty will inform Customer without undue delay if, in Requesty's opinion, an instruction from Customer infringes Applicable Data Protection Legislation, and may suspend performance of the affected instruction until Customer confirms or amends it.

5.9 Training Permitted Models. A limited number of models in the catalogue are made available by their Model Provider on terms under which that provider retains prompts and outputs and uses them to train, fine tune or otherwise improve its models, in exchange for free access. Every Training Permitted Model is made available at no charge, and no model for which Requesty charges is a Training Permitted Model. Where Requesty proposes to label a model for which it charges, it will give notice under the Terms of Service first. Requesty labels these as Training Permitted Models in the Services, in the model metadata returned by the API and at <https://requesty.ai/models>.

(a) Availability by plan. Training Permitted Models are available only on the Free Plan. Where Customer is on a Paid Plan they are excluded for Customer's organisation by default and Requesty rejects requests for them, whether or not Customer has configured Approved Models. An authorised administrator of Customer may ask Requesty in writing to make them available to Customer's organisation, and nothing is made available until Customer does so. Zero Data Retention under clause 5.3 and the EU Endpoint under clause 5.4 are not the control here and do not determine whether a Training Permitted Model is available, because those settings govern Requesty's own Processing and not the Model Provider's.

(b) Customer's instruction. Where Customer has asked Requesty in writing to make Training Permitted Models available and a user of Customer's organisation selects one, that selection is Customer's documented instruction under clause 5.1 to disclose the prompt and output content of that request to that Model Provider for the purposes stated in the provider's published terms, including training.

(c) Independent controller. In respect of its own training and model improvement purposes, the Model Provider acts as an independent controller and not as Requesty's or Customer's processor. Customer is responsible for having a lawful basis for that disclosure and for any transparency and, where required, consent obligations owed to Data Subjects.

(d) Customer responsibility. Because a Training Permitted Model retains prompts and outputs and uses them to train models, it is not suitable for Personal Data, special category data, criminal conviction data or confidential information, and Customer is responsible for assessing that before asking Requesty to make those models available and before permitting their use. Requesty makes the label available in the Services, in the model metadata returned by the API and at <https://requesty.ai/models> so that Customer can make that assessment. Absent a written request from Customer, those models remain excluded for Customer's organisation.

(e) Requesty's own use. On a Paid Plan Requesty does not use prompt or output content to train, fine tune, evaluate, benchmark or otherwise improve any model or any part of the Services, and that applies to every model in the catalogue including a Training Permitted Model. Clause 7 applies in full and without exception, and is not affected by Customer's choice of model. Requesty's own licence to use the content of requests to a Training Permitted Model applies only where the Services are used on the Free Plan, is set out in Section 6.2(a) of the Terms of Service, and is limited to operating, securing, evaluating and improving the Services, including the routing, model selection, classification and evaluation models Requesty operates as part of the Services. Requesty will not sell or licence that content in identifiable form. A Customer on a Paid Plan is not subject to that licence, including where Customer has asked for Training Permitted Models to be made available and its users select one. In that case the Model Provider trains on those requests under its own terms and Requesty does not.

■ 6. Obligations of Customer

Customer shall:

1. **Lawful basis & notice.** Ensure it has all necessary notices and lawful bases (including any required consents) to disclose the Personal Data to Requesty and for the Processing contemplated by this DPA;
2. **Accuracy & minimisation.** Provide Personal Data that is adequate, relevant, and limited to what is necessary in relation to the purposes described in Schedule 1; and
3. **Security configuration.** Use the security features of the Services (API keys, access controls, encryption, Logging settings, etc.) in accordance with the Documentation.

Customer will indemnify Requesty for losses arising from Customer's breach of this clause.

■ 7. Obligations of Requesty

Requesty shall:

1. **Process only on instructions.** Process Personal Data solely as described in this DPA and Schedule 1;
2. **Confidentiality.** Ensure that persons authorised to Process Personal Data are bound by confidentiality obligations;
3. **Security.** Implement the technical and organisational measures set out in **Schedule 3 (TOMs)** and maintain ISO 27001-aligned security controls appropriate to the risk, and not reduce the overall level of protection provided by those measures during the Term;
4. **Sub-processors.** Engage Sub-processors only in accordance with clause 8;
5. **Data Subject rights.** Taking into account the nature of the Processing, assist Customer by appropriate technical and organisational measures to respond to Data Subject requests (at Customer's cost if outside the normal functionality of the Services). Where Logging is disabled or ZDR is enabled, Requesty holds no prompt or output content and is therefore unable to search for, extract, rectify or delete such content, which Customer acknowledges is a consequence of the configuration Customer has selected;
6. **Personal Data Breach.** Notify Customer without undue delay and, in any event, within 48 hours of becoming aware of a Personal Data Breach affecting Customer Personal Data, and cooperate with Customer's reasonable remediation efforts. Notification is sent to the security and privacy contacts Customer nominates in the Order Form or, failing that, to Customer's registered administrator email address, and includes the information required by Article 33(3) to the extent then known, with further information provided in phases as the investigation progresses;
7. **No training, no model improvement, no sale.** Not (i) use Customer Personal Data, prompts, outputs or tool call content to train, fine tune, evaluate, benchmark or otherwise improve any machine learning model, whether Requesty's own or a third party's, (ii) use Customer Personal Data for any purpose other than providing and securing the Services in accordance with this DPA, or (iii) sell, rent, share or licence Customer Personal Data. This obligation is contractual, mirrors Section 6.2 of the Terms of Service and survives termination. Requesty may use aggregated statistics that contain no Personal Data and cannot reasonably be attributed to Customer or its end users. This obligation applies to content sent to every model, including a Training Permitted Model, and applies on every Paid Plan without exception. It does not

extend to a Model Provider's own use of content, which follows the model Customer selects and is addressed in clauses 5.7 and 5.9;

8. **Assistance with Articles 32 to 36.** Taking into account the nature of the Processing and the information available to Requesty, provide reasonable assistance to Customer in complying with its obligations under Articles 32 to 36 of the UK GDPR and EU GDPR, including security of Processing, notification of a Personal Data Breach to a Supervisory Authority and to Data Subjects, data protection impact assessments and prior consultation. Requesty maintains a data protection impact assessment pack, a transfer impact assessment and current security documentation at the Trust Centre;
9. **Requests received directly.** If Requesty receives a request from a Data Subject relating to Customer Personal Data, not respond to the substance of the request, refer the Data Subject to Customer, and notify Customer without undue delay;
10. **Government/law-enforcement access.** Requesty will not disclose Customer Personal Data to a public authority unless legally compelled. Where legally permitted, Requesty will promptly notify Customer, challenge unlawful or overbroad requests, and limit disclosure to the minimum required.
11. **Deletion/return.** Delete Customer Personal Data within thirty (30) days of the end of the Agreement without requiring a request from Customer and, if Customer asks before that period expires, return or export it in a commonly used machine readable format. Encrypted back-ups roll off within a further thirty five (35) days. Requesty will certify deletion in writing on request. Retention beyond these periods is permitted only where required by applicable law, in which case Requesty will store the data securely and Process it solely for that purpose; and
12. **Records & audit.** Maintain records of Processing and, once per 12-month period, provide Customer under NDA with Requesty's then current third party audit deliverables and security documentation, published at the Trust Centre, together with a summary of the most recent penetration test. Requesty's certification status, including the status of its **SOC 2 Type II** and/or **ISO 27001** programmes, is published at the Trust Centre, and Requesty makes no representation of certification beyond what is stated there. Where this documentation does not reasonably satisfy Customer's obligations under Applicable Data Protection Legislation or a Supervisory Authority requires it, Customer may conduct an audit of relevant controls on **30 days' notice**, during business hours, without disrupting operations, and at Customer's expense. Audits may be performed by Customer or an independent third party bound by confidentiality. Scope is limited to facilities, systems and records relevant to Processing of Customer Personal Data.

8. Sub-processing

8.1 **Authorised Sub-processors.** Customer authorises Requesty to engage the Infrastructure Sub-processors and Model Providers listed at

<https://requesty.ai/privacy/subprocessors>, which page distinguishes Part A (Infrastructure Sub-processors, engaged by Requesty for every customer) from Part B (Model Providers). A Model Provider is engaged only where, and to the extent that, Customer routes a request to a model operated by that provider. A Model Provider that Customer never routes to Processes no Customer Personal Data, and Customer may narrow the list applicable to it at any time by configuring Approved Models. On request Requesty will confirm in writing the sub-processors applicable to Customer's specific configuration.

8.2 Appointment & flow-down. Requesty will enter into a written agreement with each Sub-processor requiring it to meet obligations materially equivalent to those set out in this DPA.

8.3 Changes. Requesty will give Customer at least thirty (30) days' notice of any intended addition or replacement of a Sub-processor. Customer may object on reasonable data-protection grounds within that period. If the Parties are unable to resolve the objection, Customer may suspend or terminate the affected Services without penalty. Notice is given by email to the addresses Customer nominates for that purpose and by publication on the page referred to in clause 8.1, to which Customer may subscribe. Requesty will also notify Customer where Requesty becomes aware of a change to the hosting region of a model included in Customer's Approved Models, or to a Model Provider's published position on retention or on use of content for training.

8.4 Requesty remains fully liable to Customer for the performance of its Infrastructure Sub-processors' obligations. In respect of a Model Provider selected by Customer, Requesty remains responsible for conducting appropriate diligence, for putting the written terms required by clause 8.2 in place, and for accurately reproducing that provider's published data handling position, and is not liable for a Model Provider's own breach of its published terms, which Customer accepted under Section 5 of the Terms of Service when selecting the model. Nothing in this clause reduces Requesty's obligations under the SCCs where they apply.

■ 9. International Transfers

9.1 Customer Personal Data stored by Requesty is stored in Frankfurt, Germany (EEA) in all cases, regardless of endpoint choice. Where Customer elects to use the EU Endpoint (<https://router.eu.requesty.ai>), all Requesty side Processing, including routing, caching and Logging where enabled, is also performed exclusively within data centres located in the EEA. Where Customer additionally restricts Approved Models to model deployments hosted in the EEA in accordance with clause 5.4(b), no Restricted Transfer of prompt or output content arises. Where Customer uses the EU Endpoint but selects a model hosted outside the EEA, a Restricted Transfer arises at the inference layer and clause 9.3 applies.

9.2 If Customer uses a global endpoint or enables cross-region caching, Customer acknowledges that although Personal Data remains stored in Germany (EEA), Requesty and its Sub-processors may process (e.g. route and cache) Personal Data outside the UK and EEA (including in the United States) on a transient basis, subject to an appropriate transfer mechanism under Chapter V UK GDPR/EU GDPR.

9.3 Standard Contractual Clauses. Where required, the SCCs (Module 2 or 3 as applicable) and UK Addendum are incorporated into this DPA by reference as set out in **Schedule 2**.

9.4 If Requesty adopts an alternative lawful transfer mechanism (e.g. an adequacy decision

or certification scheme) that applies to the relevant transfer, that mechanism will apply instead of the SCCs. Requesty is not certified under the EU US Data Privacy Framework and does not rely on it as a transfer mechanism.

9.5 Transfer impact assessment. Requesty makes available at the Trust Centre a transfer impact assessment covering its Infrastructure Sub-processors, including the supplementary measures applied. Requesty will provide reasonable assistance to Customer in completing its own assessment in respect of the Model Providers Customer selects.

10. Liability

The liability of each Party for all claims under this DPA is subject to the limitations and exclusions of liability in the Agreement. The caps in the Agreement are aggregate caps covering claims under the Agreement and under this DPA taken together, and this DPA does not create a separate, additional or increased cap. Where the Parties have executed a Master Services Agreement, which is the usual position on an Enterprise plan, the liability provisions of that Master Services Agreement govern and prevail over this clause 10. Where the Parties have not executed a Master Services Agreement, including where Customer uses the Services on a free, self service, pay as you go or committed spend plan, the Agreement is the Requesty Terms of Service published at <https://requesty.ai/terms> and Section 18.2 of those Terms of Service governs, in the version in force at the time the claim arises. Nothing in this clause limits either Party's liability for breach of the Standard Contractual Clauses to the extent such limitation is prohibited by law, or for death or personal injury caused by negligence, or for fraud or fraudulent misrepresentation.

■ 11. Term & Termination

This DPA terminates automatically on the later of (i) deletion or return of all Personal Data by Requesty, and (ii) expiry of the Agreement. Clauses that by their nature should survive (including confidentiality, liability, and jurisdiction) shall do so.

■ 12. General

If any provision of this DPA is held invalid or unenforceable, the remainder will remain in full force. Except as amended by this DPA, the Agreement remains unchanged. In the event of conflict between this DPA and the Agreement, this DPA prevails in relation to data protection matters. This DPA is governed by the laws stated in the Agreement save where otherwise required by the SCCs.

■ 13. US State Privacy Laws

To the extent US State Privacy Laws apply to Customer Personal Data, Requesty acts as a "service provider" or "processor" and not as a "third party", does not "sell" or "share" Customer Personal Data as those terms are defined, and will not retain, use or disclose Customer Personal Data except to perform the Services or as permitted by those laws. Requesty will notify Customer if it determines that it can no longer meet these obligations.

■ 14. Contacts

Requesty's contact for data protection and security matters is privacy@requesty.ai. Requesty Ltd is established in the United Kingdom. Where Requesty is required to designate a

representative under Article 27 of the EU GDPR, the current designation is published at the Trust Centre. Customer nominates its own security and privacy contacts in the Order Form.

○ SCHEDULE 1: Processing Particulars

Item	Description
Subject-matter & Nature	Routing of Customer-supplied prompts to third-party large-language-model providers; receipt and return of model outputs; optional storage of prompts/responses; aggregation of usage metadata for billing, debugging, analytics, and security. Customer Personal Data is stored in Frankfurt, Germany (EEA) in all cases. If Customer uses the EU-only endpoint (https://router.eu.requesty.ai), all routing, caching and storage also remain within the EEA. If Customer uses global endpoints, Personal Data remains stored in Germany but transient processing (routing and caching) may occur outside the EEA. Where the model inference itself is performed is determined by the models Customer selects, as described in clause 5.4(b), and not by the endpoint Customer calls.
Purpose	Provision of the Services (LLM Router) pursuant to the Agreement; ensuring service quality, security, billing, and customer support.
Duration	As set out in the Logging Options and Retention row below. On expiry or termination of the Agreement, Customer Personal Data is deleted within 30 days and encrypted back-ups roll off within a further 35 days, in accordance with clause 7.8, unless retention is required by law.
Categories of Personal Data	Text included in prompts or model outputs that may incidentally contain Personal Data (e.g. names in free-text); user IDs or pseudonyms; device or browser metadata; usage metrics (token counts, latency, model identifier, provider region). Special category data is neither required nor expected in the standard configuration, and Customer must not include it unless the conditions in the Sensitive Data row below are met. If it is sent in error, Customer will notify Requesty without undue delay so that it can be deleted.

Data Subjects

End-users of Customer's application (e.g. employees, contractors, consumers) who submit prompts; Customer administrators; Requesty staff (logging and support metadata only).

Sensitive Data

Not anticipated or required in the standard configuration. Special category data (Article 9) and criminal conviction data (Article 10) may be Processed only where (i) Zero Data Retention is enabled for Customer's organisation under clause 5.3, (ii) Customer has a lawful basis under Article 9 or Article 10 and has completed any required assessment, and (iii) Customer restricts Approved Models to Model Providers whose published position is that they do not retain content. In every configuration, and irrespective of Zero Data Retention, Customer must not transmit children's data, government identifiers or payment card data. **If such data is sent in error, Requesty will use commercially reasonable efforts to remove it from active systems as soon as practicable after notification.**

Logging Options

Logging enabled (default on self serve plans): prompts, model outputs and metadata stored for up to 30 days in encrypted form in Frankfurt, Germany (EEA), then deleted.

Logging disabled: prompts and model outputs are not persisted at all.

Zero Data Retention (clause 5.3): no prompt or output content is written to persistent storage, and Requesty side caching is disabled.

Cache entries, where Customer enables caching: stored within the EEA and expire automatically, and are never created where Zero Data Retention is enabled.

Content free billing telemetry (token counts, model identifier, timestamp, latency, cost): retained for 6 years for statutory accounting in every configuration, including under Zero Data Retention.

Account Information (administrator names, email addresses, billing records): retained for the Term and for 6 years thereafter for statutory accounting.

○ SCHEDULE 2: Cross-Border Transfers

1. **Incorporation of SCCs (EEA/Swiss Restricted Transfers).** Where a Restricted Transfer occurs under the EU GDPR (or the Swiss FADP), the Parties agree that the European Commission Standard Contractual Clauses (Decision (EU) 2021/914) are incorporated into and form part of this DPA with the following selections:
 - Modules:
 - i. Module 1 (C2C): where the Parties transfer Account Information as independent controllers;
 - ii. Module 2 (C2P): where Customer is Controller and Requesty is Processor;
 - iii. Module 3 (P2P): where Customer is Processor and Requesty is sub-processor.
 - Clause 7: Docking clause applies.
 - Clause 9(a): Option 2 (general authorisation); 30-day prior notice of sub-processor changes.
 - Clause 11(a): Optional redress language does not apply.
 - Clause 17 (Option 1): The SCCs are governed by the laws of Ireland.
 - Clause 18(b): Disputes under the SCCs are subject to the courts of Ireland.
2. **UK Transfers.** For Restricted Transfers subject to the UK GDPR, the UK International Data Transfer Addendum (version B1.0) is incorporated. Table 1–3 information is as set out in this DPA; Table 4: neither party may terminate for updates. (Governing law and forum: England & Wales.)
3. **Swiss Transfers.** For Swiss Restricted Transfers, references to “EU Member State” are construed to Switzerland; the competent authority is the FDPIC; governing law and forum are Switzerland.
4. **Annexes.** The Annexes to the SCCs are completed as follows: Annex I.A (Parties) by the signature blocks of this DPA and the Order Form; Annex I.B (Description of the transfer) by Schedule 1; Annex I.C (Competent supervisory authority) by the supervisory authority of the EEA Member State in which Customer is established or, where Customer is not established in the EEA, the Irish Data Protection Commission; Annex II (Technical and organisational measures) by Schedule 3; and Annex III (List of Sub-processors) by the list referred to in clause 8.1. Where the SCCs conflict with any other term of this DPA, the SCCs prevail.
5. **Onward transfers.** Where Requesty transfers Customer Personal Data to a Model Provider located outside the EEA as a result of Customer’s model selection, that transfer is an onward transfer under Clause 8.8 of the SCCs and is made on the basis of the transfer mechanism in place with that Model Provider, as recorded in the list referred to in clause 8.1.

○ **SCHEDULE 3: Technical & Organisational Measures (TOMs)**

Requesty maintains an ISO 27001-aligned Information Security Management System covering:

- **Physical security:** Requesty operates no data centre of its own. Production

infrastructure is hosted by Requesty's cloud Infrastructure Sub-processors in Tier III facilities in Frankfurt, Germany (EEA), which maintain 24/7 manned security, CCTV, badge or biometric controlled access and visitor logging, evidenced by those providers' own ISO 27001 and SOC 2 reports.

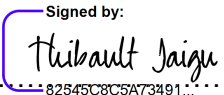
- **Network and cryptographic security:** Firewalls, private network segregation, web application firewall and DDoS protection. Encryption in transit using TLS 1.2 as a minimum and TLS 1.3 by default, with weak cipher suites disabled. Encryption at rest using AES-256. Keys are held in a managed key management service with documented rotation. Customer prompt and output content is excluded from application logs and error traces.
- **Access controls:** Access to production is role based and least privilege, granted only to named personnel. Single sign on with mandatory multi factor authentication, no shared or generic accounts, production access through a bastion host only, quarterly access reviews and revocation within 24 hours of a leaver. Access to Customer prompt and output content is restricted to a named support group, requires a ticket recording the business reason, and is logged.
- **Application and development security:** Secure development lifecycle with peer review and mandatory approval before merge, dependency and secret scanning in the pipeline, static analysis, separate development, staging and production environments with no Customer Personal Data in non production, and an annual penetration test by an independent third party with a summary available under NDA.
- **Incident response:** 24/7 on call rotation, a documented and periodically tested incident response plan with severity classification, notification to Customer within 48 hours of becoming aware of a Personal Data Breach affecting Customer Personal Data, and a written post incident review for severity 1 and severity 2 incidents.
- **Business continuity and back-ups:** Encrypted daily back-ups retained for 35 days and replicated to a second region within the EEA, with documented recovery time and recovery point objectives and recovery drills at least quarterly.
- **Vendor management:** Security due diligence and written data protection terms with all Sub-processors, an inventory reviewed at least annually, and monitoring of Model Providers' published retention and training positions, with changes reflected in the model metadata surfaced in the Services.
- **Personnel:** Mandatory annual security and privacy training, phishing simulations, background checks where permitted by law, and written confidentiality undertakings binding on all personnel and contractors that survive the end of their engagement.
- **Deletion routines:** Documented deletion routines with automated expiry of logs at the applicable retention period set out in Schedule 1, deletion of Customer Personal Data within 30 days of termination, back-up roll off within a further 35 days, and written certification of deletion on request.

■ Signatures

The Parties agree to the terms of this DPA by executing (physically or electronically) the Agreement or Order Form referencing it, or by otherwise accepting the Agreement.

Signed for and on behalf of **REQUESTY LTD**

Signed for and on behalf of

Signed by:

Signature:.....
82545C8C5A734911...
Name: Thibault Jaigu
Title: Co-Founder & Director
Date: 8/14/2026

Signature:.....
Name:
Title:
Date: