mycomplaints.ai
General Terms and Conditions v2.4

Subscribing for mycomplaints.ai via the AWS Marketplace Standard Offer:
Supplement to the AWS Marketplace Standard Contract (“SCMP”)



MYCOMPLAINTS.AI
AI COMPLAINT MANAGEMENT

General Terms and Conditions

Supplement to the AWS Marketplace Standard Contract (SCMP) when subscribing for the mycomplaints.ai Standard Offer

These General Terms and Conditions (the "General T&Cs") supplement, and form part of, the AWS Marketplace Standard Contract (the "SCMP") entered into between Mycomplaints Ltd, trading as mycomplaints.ai (the "Seller"), and the customer that accepts the SCMP via the AWS Marketplace (the "Customer"). No separate execution is required: by accepting the SCMP, the Customer also accepts these General T&Cs.

These General T&Cs address subject matter not covered by the SCMP, including the artificial intelligence and machine learning components of the Services, consumption-based usage, and the treatment of third-party AI cost changes during the Term.

These General T&Cs consist of:

- the body of these General T&Cs set out below (clauses 1 to 8);
- the Service Level Agreement (the "SLA") set out in Schedule 1; and
- the Data Processing Agreement (the "DPA") set out in Schedule 2.

Together with the SCMP, these General T&Cs form the Main Agreement. Where the Customer and the Seller have additionally accepted the mycomplaints.ai Enterprise Addendum via an AWS Marketplace Custom Offer, Order Form or other written agreement, the Enterprise Addendum also forms part of the Main Agreement.

Capitalised terms not defined in the body of these General T&Cs have the meanings given to them in the SCMP, the DPA or the SLA.

VARIABLES	
AI Sub-processors	Third-party providers of artificial intelligence, machine learning, foundation model and related cloud services used by the Seller to deliver the Services, currently the Gemini Enterprise Agent Platform, as updated from time to time in accordance with the DPA.
Excessive-Use Thresholds	Usage that materially exceeds normal or anticipated usage levels for the Customer's subscription tier, creates disproportionate consumption of third-party AI services or infrastructure resources, or adversely affects the stability, performance, availability or commercial viability of the Services.
Cost-Pass-Through Index	The greater of (a) the percentage increase in the UK Consumer Prices Index (CPI) over the relevant period and (b) five percent (5%) in any rolling twelve-month period.
Pricing Notice Period	Thirty (30) days' written notice before any cost-pass-through Fee increase takes effect.
Customer Termination Trigger	A cost-pass-through Fee increase exceeding fifteen percent (15%) of the Customer's then-current Fees in any twelve-month period.

TERMS

1. Definitions and Interpretation.

In these General T&Cs:

"AI Outputs" means outputs, recommendations, classifications, summaries, drafts and analyses generated by the artificial intelligence and machine learning components of the Services.

"AI Sub-processors" has the meaning set out in the Variables, as updated in accordance with the DPA.

"Customer Input" means any data, prompts, documents, complaint records, policies, precedents or other materials submitted by or on behalf of the Customer to the Services.

2. Nature of AI Outputs.

AI Outputs are probabilistic and may be incomplete, inaccurate, or unsuitable for the Customer's specific use case. Without limiting the warranty disclaimer in the SCMP, the Seller does not warrant that AI Outputs will be error-free, reliable, compliant with applicable laws or regulations, or fit for any particular purpose.

3. Human-in-the-Loop.

The Services may include human-in-the-loop checkpoints or review steps. These support the Customer's workflow only and do not constitute a guarantee of accuracy, completeness, fairness or compliance. The Customer is solely responsible for reviewing, validating and approving AI Outputs before relying on them, and for ensuring that any decisions, communications or actions taken on the basis of AI Outputs meet all applicable legal, regulatory and professional obligations.

4. No Delegation of Obligations.

Nothing in the Main Agreement delegates or transfers any of the Customer's legal, regulatory or professional obligations to the Seller. The Services are a tool to assist the Customer and do not replace the Customer's independent judgement, oversight or governance. The Customer shall implement and maintain appropriate policies, procedures and trained personnel to oversee the use of the Services and shall not rely on the Services as the sole basis for decisions where human judgement or regulatory oversight is required.

5. Ownership of AI Outputs.

As between the parties, the Customer retains all right, title and interest in and to Customer Input. Subject to the SCMP and the Customer's payment obligations, the Seller assigns to the Customer all right, title and interest the Seller may have in the AI Outputs generated specifically for the Customer, on the understanding that AI Outputs are not unique, may resemble outputs generated for other customers, and that similar AI Outputs may be independently generated by or for third parties. The Customer grants the Seller a worldwide, non-exclusive, royalty-free licence to host, copy, process, transmit and display Customer Input and AI Outputs solely to the extent necessary to (a) provide, secure and support the Services, (b) comply with applicable law, and (c) enforce the Seller's rights under the SCMP. The DPA governs the processing of any personal data within Customer Input and AI Outputs.

6. Usage Limits.

The Customer acknowledges that the Services use third-party AI and machine-learning services that incur variable consumption-based charges, including charges based on token usage, transaction volumes, processing requests, data volumes and related computational consumption. The Customer shall ensure that its use of the Services is fair, reasonable and proportionate to the intended use case.

Where the Seller reasonably determines that the Customer's usage meets the Excessive-Use Thresholds set out in the Variables, the Seller may, on written notice and acting reasonably and in good faith: (a) apply additional usage-based charges; (b) throttle, suspend or limit the excessive portion of usage; or (c) propose an alternative commercial arrangement. The Seller shall, where reasonably practicable, give advance notice before applying material restrictions or additional charges.

7. Cost Pass-Through to Third-Party AI Services.

The Fees are based in part on the prevailing costs of third-party AI, machine-learning, cloud-processing and related technology services used by the Seller to provide the Services. The Seller may increase the Fees during the Term where the direct costs incurred by the Seller

in obtaining such third-party services have increased by more than the Cost-Pass-Through Index set out in the Variables and that increase materially impacts the Seller's cost of providing the Services.

Any such increase shall (a) be limited to the extent reasonably necessary to reflect the increased third-party costs, (b) take effect no earlier than the Pricing Notice Period set out in the Variables and (c) be supported, on reasonable request, by sufficient evidence of the relevant cost increases on a confidential basis. If the increase reaches the Customer Termination Trigger set out in the Variables, the Customer may terminate the affected Services by written notice served within fourteen (14) days of the pricing notice; termination takes effect at the end of the then-current billing period.

8. Order of Precedence.

These General T&Cs supplement the SCMP and are taken to be amendments agreed by the parties for the purposes of clause 1.3 and clause 12.3 of the SCMP. In the event of any conflict between these General T&Cs and the SCMP (including any custom amendments, special conditions, or variations to the SCMP agreed via an AWS Marketplace Custom Offer), these General T&Cs shall prevail in respect of: (a) artificial intelligence, machine learning, AI Outputs and AI Sub-processors; (b) ownership of AI Outputs and licensing of Customer Input for AI processing; (c) AI-driven consumption-based charges and cost pass-through; (d) AI-specific disclaimers; and (e) any liability caps, indemnities, or risk allocations associated with the foregoing items (a) through (d), notwithstanding any general liability or super-cap provisions to the contrary in the SCMP. The DPA (Schedule 2) shall prevail over the body of these General T&Cs in respect of the processing of personal data, and the SLA (Schedule 1) shall prevail over the body of these General T&Cs in respect of service levels, support response times and service credits.

SCHEDULE 1 — SERVICE LEVEL AGREEMENT (SLA)

based on oneSLA v1

This Service Level Agreement (the "SLA") is Schedule 1 to, and forms part of, the General Terms and Conditions. It is based on the oneSLA standard (lawinsider.com/standards/onesla) contained within the oneSaaS suite of documents, customised for mycomplaints.ai. In the event of any conflict between this SLA and the SCMP in respect of service levels, availability, support response times or service credits, this SLA shall prevail. Capitalised terms not defined here have the meanings given to them in the SCMP, the body of the General T&Cs, or the Terms of this SLA.

Together with the body of the General T&Cs and the DPA (Schedule 2), this SLA governs the service levels applicable to the Services.

VARIABLES	
Service Availability	99.9% per calendar month, calculated as set out in the Terms.
Support Hours	9:00 AM to 5:00 PM GMT/BST (as applicable), Monday to Friday, excluding bank and public holidays in England and Wales.
Scheduled Maintenance Notice Period	5 business days' notice for planned maintenance.
Maximum Scheduled Maintenance Duration	8 hours per maintenance window, scheduled outside Support Hours wherever reasonably practicable.
Support Channels	Designated channels notified by the Seller from time to time, currently email and the in-product support portal.
Critical Issue Response Time	1 hour during Support Hours. Outside Support Hours, an engineer responds as soon as the Critical Issue is notified by our 24x7x365 automated monitoring systems.
High Issue Response Time	4 hours during Support Hours.
Medium Issue Response Time	16 hours during Support Hours.

Service Credit Thresholds	Service credits accrue against the Fees due for the affected calendar month as follows: • 98.5% – 99.89% Availability: 5% of monthly Fees • 97% – 98.49% Availability: 7.5% of monthly Fees • Less than 97% Availability: 10% of monthly Fees
Service Credit Claim Period	Within thirty (30) days of the end of the affected calendar month, failing which the right to claim service credits in respect of that month shall lapse.
Sub-processors and AI Sub-processors	As listed in Annex 2 of the DPA (Schedule 2 to the General T&Cs). Where unavailability of the Services is caused by failure of a third-party dependency outside the Seller's reasonable control, such unavailability is Excluded Downtime under the Terms.

TERMS

1. Service Availability.

The Seller commits to maintaining the Service Availability set out in the Variables during each calendar month, excluding Excluded Downtime. "Service Availability" means the percentage of total minutes in a calendar month during which the Services are available for use by the Customer, excluding Excluded Downtime, calculated as: (Total Minutes in Month − Unavailable Minutes − Excluded Downtime Minutes) ÷ (Total Minutes in Month − Excluded Downtime Minutes) × 100.

2. Scheduled Maintenance.

The Seller will give the Customer notice of scheduled maintenance in accordance with the Scheduled Maintenance Notice Period and will use reasonable endeavours to ensure that scheduled maintenance is conducted during off-peak hours and does not exceed the Maximum Scheduled Maintenance Duration set out in the Variables. Scheduled maintenance is Excluded Downtime, provided the Scheduled Maintenance Notice Period has been given.

3. Excluded Downtime.

"Excluded Downtime" means any period of unavailability of the Services caused by: (a) scheduled maintenance for which the Scheduled Maintenance Notice Period has been given; (b) Force Majeure events; (c) issues arising from the Customer's use, configuration, or network environment; (d) failure of third-party dependencies (including AI Sub-processors) outside the Seller's reasonable control; (e) service suspension due to the Customer's breach of the Main Agreement; or (f) use of non-production features or environments. Service unavailability caused by Excluded Downtime, or by actions or inactions of the Customer or third parties outside the Seller's control, does not count towards downtime calculations under this SLA.

4. Support and Response Times.

Support is available through the Support Channels set out in the Variables. The Seller will respond to support requests within the response times set out in the Variables for each severity level. The Services are monitored on a 24x7x365 basis and outside Support Hours an engineer will respond to a Critical Issue as soon as that Critical Issue is notified by the Seller's automated monitoring systems.

5. Severity.

Issue severity is determined by the Seller acting reasonably, having regard to operational impact, the number of Authorised Users affected and whether a reasonable workaround is available. A "Critical Issue" is an incident causing complete unavailability of the production Services or substantial impairment of core functionality. A "High Issue" is a significant impairment of important functionality without a reasonable workaround. A "Medium Issue" is any other defect that materially affects the Customer's use of the Services.

6. AI Outputs.

For the avoidance of doubt, AI Outputs (as defined in the body of the General T&Cs) that are unexpected, low quality, or unsuitable for a particular use case are not, of themselves, a defect or fault in the Services giving rise to a support obligation under this SLA. The probabilistic nature and limitations of AI Outputs are addressed in clauses 2 and 3 of the General T&Cs.

7. Service Integrity and Security.

The Seller will implement reasonable administrative, physical and technical measures to maintain the security, stability and integrity of the Services, including the measures set out in Annex 1 of the DPA (Schedule 2 to the General T&Cs). The Seller will promptly notify the Customer of any security breaches or service issues that materially affect the Services. Where personal data is involved, the notification timelines in the DPA apply.

8. Sub-processors and Third-Party Dependencies.

The Services depend on Sub-processors, including AI Sub-processors (as defined in the body of the General T&Cs and listed in Annex 2 of the DPA). Where unavailability of the Services is caused by failure of a third-party dependency outside the Seller's reasonable control, such unavailability is Excluded Downtime under clause 3(d).

9. Service Credits.

If Service Availability in a calendar month falls below the commitment set out in the Variables, the Customer may claim service credits in accordance with the Service Credit Thresholds. Service credits are calculated on the Fees due for the affected month and are the Customer's sole and exclusive remedy for downtime under this SLA. Service credits may not be converted to cash and may not be applied to past-due invoices. The Customer must submit a claim within the Service Credit Claim Period set out in the Variables.

10. Data Rights and Deletion.

Service credits and other remedies under this SLA do not affect the Customer's data rights set out in the body of the General T&Cs or the deletion timelines set out in the DPA, which continue to apply on and after termination of the Services.

11. Order of Precedence.

This SLA is Schedule 1 to the General T&Cs, which supplement the SCMP. In the event of any conflict between this SLA and the SCMP in respect of service levels, availability, support response times or service credits, this SLA shall prevail. The DPA (Schedule 2) shall prevail over this SLA in respect of the processing of personal data, and the body of the General T&Cs shall prevail in respect of AI Outputs and AI Sub-processors.

SCHEDULE 2 — DATA PROCESSING AGREEMENT (DPA)

based on oneDPA v1

This Data Processing Agreement (the "DPA") is Schedule 2 to, and forms part of, the General Terms and Conditions. It is based on the oneDPA standard (lawinsider.com/standards/onedpa) contained within the oneSaaS suite of documents, customised for mycomplaints.ai. Capitalised terms not defined here have the meanings given to them in the SCMP, the body of the General T&Cs, or the Terms of this DPA.

Together with the body of the General T&Cs and the SLA (Schedule 1), this DPA governs the processing of Personal Data by the Seller in connection with the Services.

PARTIES	
Controller	**Processor**
Entity details: The Customer, being the counterparty to the SCMP and signatory to the Signature Page of the Supplemental Terms. Name: As recorded in the Signature Page Address: As recorded in the Signature Page Contact: As notified by the Customer to the Seller (or, in the absence of such notification, the signatory identified on the Signature Page)	Entity details: Mycomplaints Ltd (trading as mycomplaints.ai) Registered in England and Wales Company Number: 16004977 Address: Invision House, Wilbury Way, Hitchin, England, SG4 0TY Contact: privacy@mycomplaints.ai

Execution: This DPA is Schedule 2 to the General T&Cs and forms part of the Supplemental Terms. It is executed by the Customer and the Seller by signature of the Signature Page at the front of the Supplemental Terms; no separate signature of this DPA is required.

VARIABLES	
Parties' relationship	Controller to Processor.
Parties' roles	The Customer will act as the Controller (and Business, where the CCPA/CPRA applies) as defined in Section 1 of the Terms. The Seller will act as the Processor (and Service Provider, where the CCPA/CPRA applies) as defined in Section 1 of the Terms.
Contacts	Controller contact: as notified by the Customer to the Seller, or in the absence of notification, the signatory

	identified on the Signature Page of the Supplemental Terms. Processor contact: privacy@mycomplaints.ai
Main Agreement	The AWS Marketplace Standard Contract (SCMP) entered into between the Customer and the Seller, as supplemented by the mycomplaints.ai Supplemental Terms (which consist of the General Terms and Conditions — comprising the body of the General T&Cs, the SLA at Schedule 1 and this DPA at Schedule 2 — together with the Enterprise Addendum).
Term	This DPA commences on the date of signature of the Signature Page of the Supplemental Terms by both parties and continues for the term of the Main Agreement, and thereafter for so long as the Seller processes any Personal Data on behalf of the Customer.
Breach Notification Period	Without undue delay after the Seller becomes aware of a personal data breach affecting Customer Personal Data.
Sub-processor Notification Period	30 days before the new Sub-processor is granted access to Personal Data.
Liability Cap	Each party's aggregate liability under this DPA is subject to, and forms part of, the liability caps and exclusions in the Main Agreement (including, where applicable, any sub-caps or super-caps in the SCMP, the General T&Cs or the Enterprise Addendum). Nothing in this DPA increases either party's aggregate liability beyond the caps set out in the Main Agreement.
Governing Law and Jurisdiction	As per the Main Agreement.
Data Protection Laws	All laws, regulations and court orders which apply to the processing of Personal Data in: the United Kingdom (UK); the European Economic Area (EEA); the United States (US); and Australia. This includes the European Union Regulation (EU) 2016/679 (the EU GDPR), the UK General Data Protection Regulation and the Data Protection Act 2018, the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (CCPA/CPRA), the Privacy Act 1988 (Cth) (Australia) including the Australian Privacy Principles, and any other applicable data protection or privacy laws of any jurisdiction in which the Customer is established

	or to which the Customer's processing of Personal Data is subject, in each case as amended from time to time.
Services related to processing	The mycomplaints.ai software-as-a-service solution, as described in the Main Agreement and the Seller's AWS Marketplace listing, which is used by the Customer to triage, analyse and recommend resolutions for consumer complaints, including (where applicable) complaints raised against regulated entities in the financial services and other regulated sectors.
Duration of processing	For the Term of this DPA, and thereafter only for so long as is necessary to comply with the return/deletion obligations in this DPA or with applicable law.
Nature and purpose of processing	Hosting, storage, transmission, access, retrieval, classification, summarisation, analysis and other processing operations necessary for the Seller to provide the Services to the Customer, including the use of artificial intelligence and machine-learning components (as described in the body of the General T&Cs) to triage complaints and recommend resolutions. Processing is carried out on the Customer's documented instructions, which include the Main Agreement, the Customer's use of the Services and any reasonable written instructions given by the Customer.
Personal Data	The categories of Personal Data processed are those contained in the Customer Input and AI Outputs (as defined in the body of the General T&Cs), which may include: (a) contact and identification data of complainants and other data subjects (including name, postal address, email address, telephone number, date of birth, and customer reference numbers); (b) account, transaction and financial data relating to the complaint (including account numbers, transaction history, balances, product details and correspondence with the regulated entity); (c) the content of the complaint itself and any supporting documentation provided by or on behalf of the data subject; (d) employee or agent data relating to the Customer's personnel who use the Services or whose decisions are referenced in the complaint record; and (e) any other Personal Data that the Customer chooses to submit to the Services. The Customer acknowledges that complaint records in regulated sectors (including financial services) may, by their nature, contain special category personal data (for

	example, data revealing health, ethnic origin or religious belief) or data relating to criminal offences. The Customer is responsible for the lawful basis for, and necessity of, including any such data in the Services and for implementing any additional safeguards required by Data Protection Laws.
Data subjects	The categories of data subjects include: (a) consumers and customers of the Customer (or of the regulated entity the Customer represents) who have raised, or are the subject of, a complaint; (b) authorised representatives of such consumers and customers (including legal representatives, family members and claims management companies); (c) employees, contractors and agents of the Customer who use the Services or whose actions are referenced in the complaint record; and (d) third parties referenced in the complaint record.
Special provisions	The Seller acts as a Processor and, where applicable, as a Service Provider for the purposes of the CCPA/CPRA. The Seller shall not (i) sell or share (as those terms are defined in the CCPA/CPRA) any Personal Data; (ii) retain, use or disclose Personal Data outside the direct business relationship with the Customer or for any purpose other than the specific purposes set out in this DPA; or (iii) combine Personal Data received from the Customer with Personal Data received from any other source, except as permitted by the CCPA/CPRA. The Seller certifies that it understands and will comply with these restrictions.
Transfer Mechanism	Where Personal Data is transferred from the EEA (or an adequate country with a transfer regime referencing the EU Standard Contractual Clauses) to a third country: the Standard Contractual Clauses approved by the European Commission Decision of 4 June 2021 (as amended from time to time), in the form set out in the Module 2 Schedule to this DPA. Where Personal Data is transferred from the United Kingdom to a third country: the International Data Transfer Addendum issued by the Information Commissioner's Office under Section 119A of the Data Protection Act 2018 (effective 21 March 2022), in the form set out in the IDT Addendum Schedule to this DPA. Where Personal Data is transferred from Australia or from the United States:

	such transfers shall comply with the applicable Data Protection Laws, and the parties shall co-operate in good faith to implement any additional measures reasonably required to ensure compliance, including any equivalent transfer mechanism that may be required or recommended by the competent supervisory authority.

ANNEX 1 — SECURITY MEASURES

Technical and organisational measures implemented by the Seller (as Processor) to ensure the security of Personal Data:

1. Governance and policies

- Documented information security policies, reviewed at least annually and approved by senior management.
- Defined security roles and responsibilities, including a named individual accountable for information security.
- Risk assessment and risk treatment processes covering Personal Data.
- Staff vetting, confidentiality undertakings and security awareness training on induction and at least annually.

2. Access control

- Role-based access control with least-privilege principles, applied to all production systems hosting Personal Data.
- Multi-factor authentication for all administrative and remote access to systems processing Personal Data.
- Periodic access reviews and prompt revocation on role change or termination.
- Centralised identity and authentication management, with strong password requirements and account lockout.

3. Encryption and pseudonymisation

- Encryption of Personal Data in transit using TLS 1.2 or higher.
- Encryption of Personal Data at rest using AES-256 or equivalent.
- Key management using a managed key-management service with controlled access and rotation.
- Pseudonymisation, redaction or tokenisation applied where reasonably practicable and proportionate.

4. System security and integrity

- Hardened server and workstation configurations following recognised baselines.
- Vulnerability management programme, including regular scanning and timely patching of supported components.
- Endpoint protection (anti-malware) on workstations and servers where applicable.
- Secure software development lifecycle including peer code review, secrets management and dependency scanning.

- Independent penetration testing of the Services at least annually.

5. Network and infrastructure security

- Segmented network architecture with restricted ingress/egress controls.
- Web application firewall and protections against common application-layer attacks.
- Logging, monitoring and alerting on security-relevant events, with logs retained in accordance with the Seller's retention policy.
- DDoS protection at the cloud-provider layer.

6. Physical security

- Production infrastructure is hosted in commercial cloud data centres that maintain recognised physical-security certifications (e.g. ISO 27001, SOC 2). Mycomplaints Ltd does not operate its own production data centres.
- Office premises secured by access controls, with restricted access to areas where Personal Data may be processed.

7. AI and machine-learning controls

- Contractual restrictions on AI Sub-processors prohibiting the use of Customer Input or AI Outputs to train their foundation models, except as permitted under the Main Agreement.
- Logical separation of Customer Input between tenants.
- Configuration of AI Sub-processor services to disable data-retention features (or to set them to the minimum permitted by the Sub-processor) wherever such controls are available.

8. Resilience and business continuity

- Documented business continuity and disaster recovery plans, tested at least annually.
- Regular, encrypted backups of Personal Data, with documented recovery procedures.
- Defined recovery time and recovery point objectives proportionate to the criticality of the Services.

9. Incident management

- Documented security incident response process, including triage, containment, eradication, recovery and lessons-learned phases.
- Defined escalation paths for personal data breaches and notification to the Customer in accordance with the Breach Notification Period.

10. Sub-processor and supply-chain management

- Due diligence on Sub-processors before engagement and at least annually thereafter.
- Contractual flow-down of data protection and security obligations to Sub-processors.
- Maintenance of an up-to-date register of Sub-processors (see Annex 2).

11. Return and deletion

- Documented processes for return and secure deletion of Personal Data at the end of the Term or on the Customer's written request, in accordance with this DPA.

ANNEX 2 — SUB-PROCESSORS

The Customer authorises the Seller to engage the Sub-processors listed below to process Personal Data in connection with the Services. The Seller will notify the Customer of any addition or replacement of Sub-processors in accordance with the Sub-processor Notification Period.

Sub-processor	Purpose	Categories of Personal Data	Location of processing
Amazon Web Services, Inc. (AWS)	Underlying cloud infrastructure (compute, storage, networking and managed services) used to host the Services.	All categories of Personal Data described in the Variables.	Customer-selected AWS region(s) (default: UK or EEA for UK/EU customers).
Optional (AI models used are pluggable by customers). Google LLC (Gemini Enterprise Agent Platform)	Foundation-model used to classify, summarise and reason over complaint records and to generate AI Outputs.	Customer Input submitted to the model (which may include any of the categories of Personal Data described in the Variables) and the AI Outputs generated by the model.	As configured by the Seller within the Gemini Enterprise Agent Platform; within a Customer-aligned region (EU for UK/EU customers).

The Seller's Sub-processor list may change from time to time. The Seller will notify the Customer of any proposed addition or replacement in accordance with the Sub-processor Notification Period, and the Customer may object in accordance with Section 3 (Sub-processing) of the Terms.

TERMS

1. What is this agreement about?

1.1 Purpose

The parties are entering into this Data Processing Agreement (DPA) for the purpose of processing Personal Data (as defined above).

1.2 Definitions

Under this DPA:

adequate country means a country or territory that is recognised under Data Protection Laws from time to time as providing adequate protection for processing Personal Data; and

Controller, data subject, personal data breach, process/processing, Processor and supervisory authority have the same meanings as in the Data Protection Laws; and

Business and Service Provider have the same meanings as in the CCPA/CPRA; and

Sub-Processor means another processor engaged by the Processor to carry out specific processing activities with Personal Data.

2. What are each party's obligations?

2.1 Controller obligations

The Controller instructs the Processor to process Personal Data in accordance with this DPA, and is responsible for providing all notices and obtaining all consents, licences and legal bases required to allow the Processor to process Personal Data, including in relation to any special category personal data or criminal-offence data that the Controller chooses to submit to the Services.

2.2 Processor obligations

The Processor will:

(a) only process Personal Data in accordance with this DPA and the Controller's instructions (unless legally required to do otherwise);

(b) not sell, share (within the meaning of the CCPA/CPRA), retain or use any Personal Data for any purpose other than as permitted by this DPA and the Main Agreement, and in particular will not use Personal Data for the training of any AI Sub-processor's foundation models other than as expressly permitted by the Main Agreement;

(c) inform the Controller immediately if (in its opinion) any instructions infringe Data Protection Laws;

(d) use the technical and organisational measures described in Annex 1 when processing Personal Data to ensure a level of security appropriate to the risk involved;

(e) notify the Controller of a personal data breach affecting Personal Data within the Breach Notification Period and provide assistance to the Controller as required under Data Protection Laws in responding to it;

(f) ensure that anyone authorised to process Personal Data is committed to confidentiality obligations;

(g) without undue delay, provide the Controller with reasonable assistance with:

(i) data protection impact assessments and prior consultations with supervisory authorities;

(ii) responses to data subjects' requests to exercise their rights under Data Protection Laws; and

(iii) engagement with supervisory authorities,

taking into account the nature of the processing and the information available to the Processor;

(h) if requested, provide the Controller with information necessary to demonstrate its compliance with obligations under Data Protection Laws and this DPA;

(i) allow for audits at the Controller's reasonable request, provided that audits are limited to once a year and during business hours, give reasonable prior notice, respect the confidentiality of other customers and the Processor's systems, and except that more frequent audits may be conducted following a personal data breach. The Controller may accept the Processor's most recent independent third-party audit reports (such as SOC 2 or ISO 27001 reports) in satisfaction of audit requests, to the extent they cover the relevant subject matter; and

(j) return Personal Data upon the Controller's written request, or delete Personal Data by the end of the Term, unless retention is legally required.

2.3 Warranties

The parties warrant that they and any staff and/or subcontractors will comply with their respective obligations under Data Protection Laws for the Term.

3. Sub-processing

3.1 Use of Sub-processors

The Controller authorises the Processor to engage other processors (referred to in this section as Sub-processors) when processing Personal Data. The Processor's existing Sub-processors are listed in Annex 2.

3.2 Sub-processor requirements

The Processor will:

(a) require its Sub-processors to comply with terms equivalent to the Processor's obligations in this DPA;

(b) ensure appropriate safeguards are in place before internationally transferring Personal Data to a Sub-processor; and

(c) be liable for any acts, errors or omissions of its Sub-processors as if they were a party to this DPA, subject to the Liability Cap in the Variables and the liability provisions of the Main Agreement.

3.3 Approvals

The Processor may appoint new Sub-processors provided that it notifies the Controller in writing in accordance with the Sub-processor Notification Period.

3.4 Objections

The Controller may reasonably object in writing to any future Sub-processor on data protection grounds. If the parties cannot agree on a solution within a reasonable time, either party may terminate the affected portion of the Services. Where termination relates to a Sub-processor whose services are integral to the Services, the Processor may instead, at its option, terminate the Main Agreement in respect of the affected Services.

4. International personal data transfers

4.1 Instructions

The Processor will transfer Personal Data outside the UK, the EEA or an adequate country only on documented instructions from the Controller, unless otherwise required by law. The Customer's execution of the Supplemental Terms, together with its use of the Services and (where applicable) its selection of Service regions, constitutes its documented instructions for such transfers.

4.2 Transfer mechanism

Where a party is located outside the UK, the EEA or an adequate country and receives Personal Data:

(a) that party will act as the data importer;

(b) the other party is the data exporter; and

(c) the relevant Transfer Mechanism set out in the Variables will apply, as completed by the Module 2 Schedule and the IDT Addendum Schedule below.

4.3 Additional measures

If the Transfer Mechanism is insufficient to safeguard the transferred Personal Data, the data importer will promptly implement supplementary measures to ensure Personal Data is protected to the same standard as required under Data Protection Laws.

4.4 Disclosures

Subject to the terms of the relevant Transfer Mechanism, if the data importer receives a request from a public authority to access Personal Data, it will (if legally allowed):

(a) challenge the request and promptly notify the data exporter about it; and

(b) only disclose to the public authority the minimum amount of Personal Data required and keep a record of the disclosure.

5. Other important information

5.1 Survival

Any provision of this DPA which is intended to survive the Term will remain in full force.

5.2 Order of precedence

This DPA is Schedule 2 to the General T&Cs, which supplement the SCMP, and is taken to be an amendment agreed by the parties for the purposes of clause 1.3 and clause 12.3 of the SCMP. In case of a conflict between the documents that form part of the Main Agreement and any applicable transfer mechanism, they will take priority in this order:

(a) the Transfer Mechanism (the Module 2 Schedule and/or IDT Addendum Schedule);

(b) this DPA;

(c) the body of the General T&Cs (save that this DPA prevails over the body of the General T&Cs in respect of the processing of Personal Data);

(d) the SLA (Schedule 1); and

(e) the SCMP.

5.3 Notices

Formal notices under this DPA must be in writing and sent to the contact details set out in the Parties table at the front of this DPA, as may be updated by a party to the other in writing.

5.4 Third parties

Except for affiliates and (where applicable) data subjects to the extent provided in the Transfer Mechanism, no one other than a party to this DPA has the right to enforce any of its terms.

5.5 Entire agreement

This DPA, together with the other documents forming part of the Main Agreement, supersedes all prior discussions and agreements and constitutes the entire agreement between the parties with respect to the processing of Personal Data, and neither party has relied on any statement or representation of any person in entering into this DPA.

5.6 Amendments

Any amendments to this DPA must be agreed in writing. The Seller may update Annex 1 (Security measures) and Annex 2 (Sub-processors) from time to time provided that no such update shall materially reduce the level of protection afforded to Personal Data.

5.7 Assignment

Neither party can assign this DPA to anyone else without the other party's consent, except that the Seller may assign this DPA as part of an assignment of the Main Agreement.

5.8 Waiver

If a party fails to enforce a right under this DPA, that is not a waiver of that right at any time.

5.9 Governing law and jurisdiction

The Governing Law and Jurisdiction set out in the Variables apply to this DPA and all disputes will only be litigated in the courts of that Jurisdiction.

MODULE 2 SCHEDULE — EU STANDARD CONTRACTUAL CLAUSES (CONTROLLER TO PROCESSOR)

Purpose. This Schedule supplements this DPA to govern the international transfer of Personal Data from the EEA (or an adequate country with a transfer regime referencing the EU SCCs) to a third country. By signature of the Signature Page of the Supplemental Terms, the parties agree to the terms of this Schedule.

Parties

Data exporter: the Customer (Controller), as identified in the Parties table at the front of this DPA.

Data importer: the Seller (Processor), Mycomplaints Ltd trading as mycomplaints.ai, as identified in the Parties table at the front of this DPA.

Variables to the Clauses

VARIABLES	
Docking	Clause 7 of the Clauses applies.
Use of Sub-processors	No changes are made to Clause 9 in the Clauses. Option 2 (General written authorisation) applies: the data importer has the data exporter's general authorisation for the engagement of Sub-processor(s) from the list set out in Annex 2 of the DPA / Annex III of this Schedule. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of Sub-processors in accordance with the Sub-processor Notification Period.
Redress	No changes are made to Clause 11 in the Clauses.
Supervision	No changes are made to Clause 13(a) in the Clauses.
Governing law	These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of the Republic of Ireland.

Annex I to the Clauses

A. List of parties – as described in the Parties table at the front of this DPA. The data exporter's role is Controller; the data importer's role is Processor.

B. Description of transfer – as described in the Variables table at the front of this DPA. Transfer frequency: continuous, for the duration of the Term. Retention period: for the duration of the Term and thereafter only for so long as is necessary to comply with the return/deletion obligations in this DPA or with applicable law. Sub-processor transfers: as described in Annex 2 of this DPA.

C. Competent supervisory authority – the supervisory authority of the EU Member State in which the data exporter is established, or, where the data exporter is not established in the EU, the supervisory authority of the EU Member State in which the data exporter's representative (appointed under Article 27 of the EU GDPR) is established, or, in the absence of such representative, the supervisory authority of an EU Member State in which the data subjects are located. The Irish Data Protection Commission shall act as the competent supervisory authority where no other supervisory authority is competent.

Annex II to the Clauses — Technical and organisational measures

As described in Annex 1 of this DPA.

Annex III to the Clauses — List of Sub-processors

As described in Annex 2 of this DPA.

IDT ADDENDUM SCHEDULE — UK INTERNATIONAL DATA TRANSFER ADDENDUM

Purpose. This Schedule supplements this DPA to govern the international transfer of Personal Data from the United Kingdom to a third country. By signature of the Signature Page of the Supplemental Terms, the parties agree to the terms of this Schedule, which forms the UK International Data Transfer Addendum to the EU Standard Contractual Clauses set out in the Module 2 Schedule above.

Part 1: Tables

Table 1 — Parties

Start date: the date of signature of the Signature Page of the Supplemental Terms by both parties.

Exporter (who sends the Restricted Transfer): the Customer (Controller), as identified in the Parties table at the front of this DPA.

Importer (who receives the Restricted Transfer): the Seller (Processor), Mycomplaints Ltd trading as mycomplaints.ai, as identified in the Parties table at the front of this DPA.

Key contacts: as set out in the Parties table at the front of this DPA.

Signatures: this Schedule is executed by the signature of the Signature Page of the Supplemental Terms by both parties; no separate signature of this Schedule is required.

Table 2 — Selected SCCs, Modules and selected clauses

Addendum EU SCCs: the EU Standard Contractual Clauses approved by the European Commission Decision of 4 June 2021 (as amended from time to time), Module 2 (Controller to Processor), as completed by the Module 2 Schedule to this DPA, including the Appendix Information.

Table 3 — Appendix Information

VARIABLES	
Annex 1A — List of Parties	As described in the Module 2 Schedule to this DPA.
Annex 1B — Description of Transfer	As described in the Module 2 Schedule to this DPA.
Annex II — Technical and organisational measures	As described in Annex 1 of this DPA.
Annex III — List of Sub-processors	As described in Annex 2 of this DPA.

Table 4 — Ending this Addendum when the Approved Addendum changes

Which Parties may end this Addendum as set out in Section 19: neither party.

Part 2: Mandatory Clauses

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses. The Mandatory Clauses are incorporated into this Schedule by reference and apply in full as published by the Information Commissioner's Office.