OMNICHAT DATA PROCESSING ADDENDUM

This **Data Processing Addendum** ("**DPA**") forms part of the **Agreement** between **OmniChat** and **Customer** and sets out the terms that apply to the processing of **Personal Data** by **OmniChat** on behalf of **Customer** in connection with the provision of the **Services**.

1. DEFINITIONS

In this **Data Processing Addendum** ("**DPA**"), the following terms shall have the meanings set forth below:

1.1 "**Agreement**" means the main service **Agreement** between **OmniChat** and **Customer** governing the provision of the **Services**.

1.2 "**AI Models**" means the third-party artificial intelligence language models accessible through the **Services**, including but not limited to GPT-4o, Claude, and Gemini.

1.3 "**Customer**" means the entity that has entered into the **Agreement** with **OmniChat** for the provision of the **Services**.

1.4 "**Customer Data**" means any **Personal Data** that **Customer** provides to **OmniChat** or that **OmniChat** processes on behalf of **Customer** in connection with the **Services**.

1.5 "**Data Controller**" (or "**Controller**") means the entity which determines the purposes and means of the **Processing** of **Personal Data**. For the purposes of this **DPA**, **Customer** is the **Data Controller**.

1.6 "**Data Processor**" (or "**Processor**") means the entity which **Processes Personal Data** on behalf of the **Data Controller**. For the purposes of this **DPA**, **OmniChat** is the **Data Processor**.

1.7 **"Data Protection Laws"** means all applicable laws relating to data protection and privacy including, without limitation, the UK GDPR, the Data Protection Act 2018 and the EU GDPR, as amended or replaced from time to time.

1.8 "**Data Subject**" means the identified or identifiable natural person to whom **Personal Data** relates.

1.9 "**Personal Data**" means any information relating to an identified or identifiable natural person processed as part of the **Services**.

1.10 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to **Customer Data**.

1.11 "**Processing**" means any operation performed on **Personal Data**, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.12 "**Services**" means **OmniChat**'s secure interface providing access to **AI Models**, including all related features and functionalities, professional **Services**, and support **Services**.

1.13 "**SubProcessor**" means any **Processor** engaged by **OmniChat** to assist in fulfilling its obligations with respect to providing the **Services**.

1.14 "**Supervisory Authority**" means an independent public authority established pursuant to Article 51 of the EU GDPR or Article 51 of the UK GDPR.

1.15 "**User**" means an individual authorised by **Customer** to use the **Services**.

2. SCOPE & PURPOSE

2.1 Application of this DPA

This **DPA** applies to the **Processing** of **Customer Data** by **OmniChat** on behalf of **Customer** in the course of providing the **Services** and forms an integral part of the **Agreement** between **OmniChat** and **Customer**.

2.2 Nature of Processing

OmniChat shall **Process Customer Data** solely for the following purposes:
(a) Providing and maintaining the **Services**, including:
- **User** authentication and access management
- Facilitating interactions with **AI Models**
- Storing and retrieving conversation history
- Managing custom prompts and workflows
- Generating exports in supported formats

(b) Technical support and problem resolution
(c) Service optimisation and improvement
(d) Security monitoring and threat detection
(e) Compliance with legal obligations

2.3 Duration of Processing

OmniChat shall **Process Customer Data** for the duration of the **Agreement**, except where:
(a) A longer retention period is required by applicable law
(b) **Customer** has provided specific written instructions for earlier deletion
(c) The data has been anonymised in accordance with Section 2.4

2.4 Data Retention

2.4.1 **OmniChat** shall retain **Customer Data** as follows:

(a) Conversation data: For the duration of the **Agreement**, unless earlier deleted by **Customer** through the **OmniChat** user interface. Note that deleted conversations may remain in database backups for up to 8 days
(b) Database backups: Maximum of eight (8) days
(c) Authentication logs: Maximum of thirty (30) days

2.4.2 Upon termination of the **Agreement**, **OmniChat** shall either delete or return **Customer Data** in accordance with Section 10 of this **DPA**.

2.4.3 **SubProcessor** Data Retention and Model Training

2.4.3.1 No Training of **AI Models**

(a) **OmniChat** ensures **Customer Data** is not utilised for general **AI Model** training purposes by any **AI Model** providers
(b) This forms a core requirement in **OmniChat**'s selection of **AI Model** providers
(c) **OmniChat** regularly reviews provider documentation and agreements to verify compliance

2.4.3.2 Limited Data Usage

(a) Customer acknowledges that **AI Model** providers may retain and process certain data:
- For security and abuse prevention
- To comply with applicable laws
- As specified in their respective Data Processing Addendums

2.4.3.3 Provider Agreements:

(a) Current **AI Model** provider Data Processing Addendums are available at:
- OpenAI: openai.com/policies/data-processing-addendum
- Anthropic: anthropic.com/legal/commercial-terms
- Google: business.safety.google/processorterms
- Perplexity: perplexity.ai/hub/legal/perplexity-api-terms-of-service

2.4.3.4 Monitoring and Updates

(a) **OmniChat** shall:
- Monitor provider data processing policies
- Notify **Customers** of material changes within 30 days
- Take appropriate action to maintain data privacy
- Provide **Customers** opportunity to object to material changes

2.4.3.5 Third-Party Compliance

(a) Customer's use of the **Services** is subject to **OmniChat**'s policies. Customer is not required to enter into separate terms with AI Model providers; OmniChat engages such providers as SubProcessors under written agreements
(b) **OmniChat** shall assist **Customers** in addressing provider policy breaches
(c) **OmniChat** shall notify the **Customer** of any known unauthorised access to or misuse of Customer Data by SubProcessors and provides reasonable assistance in mitigating such issues.
(d) **OmniChat** will provide reasonable assistance in mitigating provider data misuse

2.5 Categories of Personal Data

The types of **Personal Data** that may be **Processed** under this **DPA** include:
(a) **User** account information (names, email addresses, authentication data)
(b) Usage data (interaction logs, usage patterns, preferences)
(c) Any **Personal Data** contained within **Customer**'s interactions with the **AI Models**

2.6 Categories of Data Subjects

The categories of **Data Subjects** whose **Personal Data** may be **Processed** under this **DPA** include:
(a) **Customer**'s authorised **Users**
(b) **Customer**'s employees and contractors
(c) Any other individuals whose **Personal Data** is contained within **Customer**'s interactions with the **Services**

2.7 Geographic Scope

2.7.1 **OmniChat** shall **Process** and store **Customer Data** within the European Union, specifically:
(a) Frontend **Services**: United Kingdom
(b) Database **Services**: Belgium

2.7.2 Any transfer of **Customer Data** outside these locations shall occur only in accordance with Section 8 of this **DPA** (International Transfers).

3. ROLES & RESPONSIBILITIES

3.1 Data Controller (Customer)

3.1.1 **Customer**, as **Data Controller**, shall:
(a) Ensure it has all necessary rights, permissions, and consents to **Process Personal Data** through the **Services**
(b) Comply with all applicable **Data Protection Laws** in its use of the **Services**
(c) Provide clear and documented instructions to **OmniChat** regarding the **Processing** of **Customer Data**
(d) Be responsible for the accuracy, quality, and legality of **Customer Data**
(e) Implement appropriate technical and organisational measures to ensure the security of its access credentials
(f) Notify **OmniChat** promptly of any unauthorised access or security incidents it becomes aware of

3.2 Data Processor (OmniChat)

3.2.1 **OmniChat**, as **Data Processor**, shall:
(a) **Process Customer Data** only on documented instructions from **Customer**
(b) Maintain appropriate technical and organisational security measures as detailed in Section 5
(c) Assist **Customer** in responding to **Data Subject** requests
(d) Support **Customer** in ensuring compliance with its obligations under **Data Protection Laws**
(e) Notify Customer without undue delay, and in any event within forty-eight (48) hours, upon becoming aware of a confirmed **Personal Data Breach**
(f) Maintain records of all **Processing** activities carried out on behalf of **Customer**

3.3 Confidentiality

3.3.1 **OmniChat** shall:

(a) Ensure that all personnel authorised to **Process Customer Data** are subject to binding confidentiality obligations
(b) Limit access to **Customer Data** to those personnel who require such access to perform the **Services**
(c) Provide appropriate training to personnel on data protection and security requirements

3.4 SubProcessing

3.4.1 **OmniChat** may engage **SubProcessors** in accordance with Section 6 of this **DPA**, provided that:

(a) **OmniChat** remains fully liable for all obligations subcontracted to **SubProcessors**
(b) **SubProcessors** are bound by written agreements that require them to provide at least the level of data protection required by this **DPA**

3.5 Cooperation and Support

3.5.1 **OmniChat** shall provide reasonable assistance to **Customer** in:

(a) Responding to **Data Subject** requests
(b) Implementing security measures
(c) Conducting data protection impact assessments
(d) Consulting with Supervisory Authorities
(e) Demonstrating compliance with **Data Protection Laws**

3.6 Instructions

3.6.1 **OmniChat** shall:

(a) **Process Customer Data** only in accordance with **Customer**'s documented instructions
(b) Immediately inform **Customer** if, in **OmniChat**'s opinion, an instruction infringes **Data Protection Laws**
(c) Maintain records of all **Processing** instructions received from **Customer**

3.7 Compliance Demonstration

3.7.1 **OmniChat** shall:

(a) Maintain documentation of its security measures and data processing activities
(b) Allow for and contribute to audits and inspections as detailed in Section 9
(c) Inform **Customer** if it becomes aware of any circumstance that may affect its ability to comply with this **DPA**

4. PROCESSING REQUIREMENTS

4.1 Lawful Processing

4.1.1 **OmniChat** shall:

(a) **Process Customer Data** only in accordance with this **DPA** and the **Agreement**
(b) Ensure all **Processing** activities comply with applicable **Data Protection Laws**
(c) Not **Process Customer Data** for any purpose other than those specified in Section 2.2
(d) Not sell, rent, trade, or otherwise commercially exploit **Customer Data;**
(e) Maintain documentation of all **Processing** activities as required by **Data Protection Laws**

4.2 Processing Restrictions

4.2.1 **OmniChat** shall not:

(a) **Process Customer Data** beyond what is necessary to provide the **Services**
(b) Use **Customer Data** to train or improve **AI Models**
(c) Combine **Customer Data** with other data sources unless explicitly authorised in writing
(d) Retain **Customer Data** beyond the periods specified in Section 2.4
(e) Transfer **Customer Data** outside the specified geographic locations except as permitted under Section 8

4.3 Processing Controls

4.3.1 **OmniChat** shall implement controls to ensure:

(a) Separation of **Customer Data** between different **Customers**
(b) Prevention of unauthorised access, copying, or transmission
(c) Logging of all **Processing** activities
(d) Proper handling of export requests in supported formats (PNG, TXT, MD, JSON, CSV)
(e) Secure deletion of **Customer Data** when required

4.4 Quality and Transparency

4.4.1 **OmniChat** shall:

(a) Maintain the integrity and quality of **Customer Data** during **Processing**
(b) Provide transparent information about **Processing** activities
(c) Alert **Customer** to any significant changes in **Processing** operations
(d) Document all **Processing** activities in a clear and accessible manner

4.5 Special Categories of Data

4.5.1 **OmniChat**:

(a) Is not intended to **Process** special categories of **Personal Data**
(b) Shall notify **Customer** if it becomes aware that special categories of **Personal Data** are being **Processed**
(c) May implement additional safeguards if special categories of **Personal Data** are identified

4.6 Data Minimisation

4.6.1 **OmniChat** shall:

(a) **Process** only **Customer Data** that is necessary for the provision of the **Services**
(b) Implement measures to minimise the collection of unnecessary **Personal Data**
(c) Support **Customer** in implementing data minimisation principles

4.7 Processing Records

4.7.1 **OmniChat** shall maintain records of:

(a) Categories of **Processing** activities carried out
(b) Transfers of **Customer Data** to third countries
(c) Technical and organisational security measures implemented
(d) **Personal Data Breaches** and remedial actions taken
(e) Requests from **Data Subjects** and responses provided

4.8 Technical Integration

4.8.1 **OmniChat** shall ensure:

(a) Secure integration with supported **AI Models**
(b) Proper handling of API authentication and data transmission
(c) Appropriate error handling and failure recovery
(d) Monitoring of **Processing** performance and reliability

4.9 Processing Changes

4.9.1 **OmniChat** shall:

(a) Notify **Customer** of any intended changes to **Processing** operations
(b) Obtain **Customer**'s approval for significant **Processing** changes
(c) Document all changes to **Processing** operations
(d) Update **Processing** records to reflect any changes

5. SECURITY MEASURES

5.1 General Security Standards

5.1.1 **OmniChat** shall implement and maintain appropriate technical and organisational measures to protect **Customer Data** against unauthorised or unlawful **Processing** and against accidental loss, destruction, damage, alteration, or disclosure. Such measures shall include, at a minimum:

5.2 Technical Security Measures

5.2.1 Encryption and Data Protection:

(a) Encryption of **Customer Data** at rest using AES-256
(b) TLS 1.2 or higher for all data in transit
(c) Secure key management systems
(d) Regular encryption protocol reviews and updates

5.2.2 Access Control:

(a) Multi-factor authentication (MFA) for all administrative and infrastructure access
(b) Support for Single Sign-On (SSO) integration
(c) Role-based access control (RBAC)
(d) Unique **User** identifiers
(e) Automatic session timeout
(f) Regular access rights review

5.2.3 Network Security:

(a) Firewall protection and network segregation
(b) IP-based access control restricting database connections to authorised servers only
(c) Regular security patching and updates
(d) Network monitoring and logging
(e) Secure API connections to service providers

5.2.4 Infrastructure Security:

(a) Cloud hosting on Google Cloud Platform
(b) Database hosting on MongoDB Atlas
(c) Separate production and non-production environments
(d) Regular security assessments and penetration testing
(e) Automated backup systems with 8-day retention

5.3 Organisational Security Measures

5.3.1 Personnel Security:

(a) Confidentiality agreements with all personnel
(b) Security awareness training
(c) Access granted on a need-to-know basis
(d) Documented security procedures
(e) Regular security policy reviews

5.3.2 Security Policies and Procedures:

(a) Documented security policies
(b) Incident response procedures
(c) Change management processes
(d) Regular policy reviews and updates
(e) Security compliance monitoring

5.4 Physical Security

5.4.1 Infrastructure Security:

(a) Cloud services provided by Google Cloud Platform
(b) Database services provided by MongoDB Atlas (hosted by Google Cloud Platform)
(c) Industry-standard physical security through cloud providers
(d) Environmental controls through cloud providers
(e) Redundant power and connectivity through cloud providers

5.5 Security Monitoring and Incident Response

5.5.1 Monitoring:

(a) Regular security log review
(b) Automated threat detection through cloud provider services
(c) Security log collection and analysis
(d) Regular security testing and vulnerability scanning
(e) Performance and availability monitoring

5.5.2 Incident Response:

(a) Documented incident response procedures
(b) Clear escalation paths and response roles
(c) **Customer** notification procedures
(d) Post-incident analysis and reporting
(e) Regular review of incident response procedures

5.6 Business Continuity and Disaster Recovery

5.6.1 Business Continuity:

(a) Business continuity plan
(b) Regular backup testing
(c) System redundancy
(d) Failover procedures
(e) Service availability monitoring

5.7 Security Documentation and Compliance

5.7.1 Documentation:

(a) Security architecture documentation
(b) System configuration documentation
(c) Security procedure documentation
(d) Audit logs and reports
(e) Compliance documentation

5.8 Security Updates and Reviews

5.8.1 Regular Review and Update of:

(a) Security measures and controls
(b) Risk assessments
(c) Security policies and procedures
(d) Security training materials
(e) Incident response procedures

5.9 Third-Party Security

5.9.1 **SubProcessor** Security:

(a) **OmniChat** engages only **SubProcessors** who:
- Maintain appropriate security certifications

- Implement encryption for data in transit and at rest
- Provide documented security measures
- Have incident response procedures

(b) **OmniChat** maintains:

- Copies of **SubProcessor** Data Processing Addendums
- Current security documentation from each provider
- Records of security incident notifications

(c) Current **SubProcessor** security documentation is available at:

- OpenAI: trust.openai.com
- Anthropic: trust.anthropic.com
- Perplexity: trust.perplexity.ai
- Google Cloud: cloud.google.com/trust-center
- MongoDB Atlas: mongodb.com/products/platform/trust

(d) **OmniChat** monitors **SubProcessor** security updates and incident notifications

(e) **OmniChat** will notify **Customers** of any reported security incidents from **SubProcessors** that may affect **Customer Data**

6. SUBPROCESSOR MANAGEMENT

6.1 General Authorisation

6.1.1 **Customer** provides **OmniChat** with general authorisation to engage **SubProcessors**, subject to the conditions set forth in this Section.

6.2 Current SubProcessors

6.2.1 **OmniChat**'s current **SubProcessors** include:

(a) OpenAI - AI model provider (GPT-4o/4o mini/ o3-mini)

(b) Anthropic - AI model provider (Claude)

(c) Perplexity - AI model provider (Sonar)

(d) Google - Cloud infrastructure and AI model provider (Gemini)

(e) MongoDB Atlas - Database services, hosted on Google Cloud

6.3 SubProcessor Requirements

6.3.1 **OmniChat** shall:

(a) Conduct appropriate due diligence on all potential **SubProcessors**

(b) Enter into written agreements with **SubProcessors** that include data protection obligations no less protective than those in this **DPA**

(c) Remain liable for the acts and omissions of its **SubProcessors** to the same extent **OmniChat** would be liable if performing the services itself, provided that **OmniChat** shall not be liable for a **SubProcessor's** breach where **OmniChat** demonstrates that it:

(i) conducted appropriate due diligence prior to engaging the **SubProcessor**;

(ii) entered into written agreements containing data protection obligations no less protective than those in this DPA;

(iii) monitored the **SubProcessor's** compliance with its data protection obligations; and

(iv) promptly notified **Customer** and took reasonable steps to mitigate harm upon becoming aware of the breach.
(d) Maintain an up-to-date list of all **SubProcessors**
(e) Monitor **SubProcessor** compliance with data protection obligations

6.3.2 Industry-Standard Providers

Customer acknowledges that the **SubProcessors** listed in Section 6.2 (including OpenAI, Anthropic, Google, and MongoDB Atlas) represent industry-standard providers with established security certifications and data protection practices. **Provider's** selection of these **SubProcessors** constitutes reasonable due diligence. Claims arising from the acts or omissions of such **SubProcessors** shall be subject to the limitation of liability in the main Agreement and shall not, of themselves, constitute gross negligence or wilful misconduct by **Provider**.

6.3.3 Insurance

Provider maintains:

(a) **Professional Indemnity Insurance** with coverage of not less than £1,000,000 per claim; and

(b) **Cyber and Data Insurance** with coverage of not less than £100,000 per claim.

Provider shall maintain such coverage (or substantially equivalent coverage) for the duration of this Agreement.

Evidence of coverage shall be provided upon **Customer's** reasonable request.

6.4 New SubProcessors

6.4.1 Before engaging any new **SubProcessor**, **OmniChat** shall:

(a) Assess the **SubProcessor**'s security measures and compliance capabilities

(b) Provide **Customer** with at least thirty (30) days' prior written notice

(c) Include the new **SubProcessor**'s details in the **SubProcessor** List

(d) Ensure the new **SubProcessor** is bound by appropriate contractual terms

6.5 SubProcessor List

6.5.1 **OmniChat** shall:

(a) Maintain a current list of **SubProcessors** as detailed in Section 6.2

(b) Notify **Customer** of any changes to **SubProcessors** in accordance with Section 6.4

(c) Document all **SubProcessor** details including:

- Name and location of each **SubProcessor**
- Description of **Processing** activities
- Categories of **Customer Data** processed
- Security measures implemented

6.6 Customer Objection Rights

6.6.1 **Customer** may object to a new **SubProcessor** by providing written notice to OmniChat within thirty (30) days of notification, stating reasonable grounds relating to data protection.

6.6.2 If **Customer** objects, **OmniChat** shall:

(a) Work with **Customer** to address the objection

(b) Where possible, provide alternative options to **Customer**, including:

- Maintaining the **Services** without the proposed **SubProcessor**
- Suggesting a different **SubProcessor**
- Modifying the **Services** to avoid the need for the **SubProcessor**

6.6.3 If no resolution is possible, either party may terminate the affected **Services** without penalty upon written notice to the other party.

6.7 Emergency Replacement

6.7.1 **OmniChat** may replace a **SubProcessor** without prior notice where urgent replacement is required to:

(a) Maintain service continuity

(b) Address security vulnerabilities
(c) Comply with legal requirements

6.7.2 In such cases, **OmniChat** shall:

(a) Notify **Customer** as soon as practicable
(b) Provide **Customer** with the right to object retrospectively
(c) Work with **Customer** to address any concerns

6.8 SubProcessor Monitoring

6.8.1 **OmniChat** shall:

(a) Regularly monitor and review **SubProcessor** performance
(b) Conduct periodic security assessments
(c) Verify compliance with contractual obligations
(d) Maintain records of all monitoring activities
(e) Address any identified issues promptly

6.9 SubProcessor Changes

6.9.1 **OmniChat** shall:

(a) Document all changes to **SubProcessor** arrangements
(b) Update security and privacy documentation accordingly
(c) Maintain records of previous **SubProcessor** relationships
(d) Ensure proper transition of **Services** between **SubProcessors**

7. DATA SUBJECT RIGHTS

7.1 General Obligations

7.1.1 **OmniChat** shall assist **Customer** in fulfilling its obligations to respond to **Data Subject** requests under applicable **Data Protection Laws**, including requests to:

(a) Access Personal Data
(b) Rectify inaccurate **Personal Data**
(c) Erase **Personal Data** ("right to be forgotten")
(d) Restrict or object to **Processing**
(e) Export **Personal Data** ("data portability")

7.2 Data Subject Request Process

7.2.1 Upon receiving a **Data Subject** request directly, **OmniChat** shall:

(a) Notify **Customer** within five (5) business days of receiving the request;
(b) Not respond directly to the **Data Subject**
(c) Provide **Customer** with all necessary information
(d) Follow **Customer**'s reasonable instructions
(e) Maintain records of all requests received

7.2.2 Upon receiving a request from **Customer** regarding a **Data Subject** request, **OmniChat** shall:

(a) Acknowledge receipt within 2 business days
(b) Provide initial response and assistance within five (5) business days of receiving **Customer's** instruction;
(c) Complete request within reasonable timeframe based on complexity
(d) Keep **Customer** informed of progress for complex requests
(e) Confirm completion to **Customer**

7.3 Technical Measures

7.3.1 **OmniChat** shall maintain technical capabilities to:

(a) Search for specific **Data Subject** information
(b) Export **Personal Data** in common formats (JSON, CSV, TXT)
(c) Modify or delete **Personal Data** as required
(d) Maintain audit trails of all actions
(e) Implement technical restrictions on **Processing** when requested

7.4 Response Timeframes

7.4.1 **OmniChat** shall:

(a) Acknowledge receipt of requests within 2 business days
(b) Provide initial response within five (5) business days;
(c) Complete standard requests within reasonable timeframe based on complexity
(d) Provide regular status updates for complex requests
(e) Meet statutory timeframes as required by **Data Protection Laws**

7.5 Data Export Capabilities

7.5.1 **OmniChat** provides continuous self-service export capabilities through its user interface, allowing **Users** to:

(a) Export their data at any time
(b) Choose from multiple formats including:
  - JSON (machine-readable)
  - CSV (structured data)
  - Markdown (formatted text)
  - TXT (plain text)
  - PNG (visual records)
(c) Export complete conversation message history
(d) Include relevant metadata and timestamps
(e) Access exports in a structured and organised manner

7.5.2 These export capabilities:

(a) Are available throughout the duration of the **Agreement**
(b) Require no additional assistance from **OmniChat**
(c) Can be performed as frequently as needed
(d) Support **Data Subject** rights under applicable **Data Protection Laws**

7.6 Verification and Authentication

7.6.1 **OmniChat** shall:

(a) Verify the authenticity of **Customer** requests
(b) Implement secure communication channels
(c) Maintain authentication records
(d) Follow agreed security protocols
(e) Report suspicious requests to **Customer**

7.7 Special Circumstances

7.7.1 **OmniChat** shall have procedures for handling:

(a) Urgent requests involving **Data Subject** rights
(b) Requests affecting multiple **Data Subjects**
(c) Complex or unusual requests
(d) Requests involving multiple jurisdictions
(e) Requests requiring special handling

7.8 Documentation and Records

7.8.1 **OmniChat** shall maintain records of:

(a) All **Data Subject** requests received
(b) Actions taken in response
(c) Communication with **Customer**
(d) Timeframes for completion
(e) Any issues or complications encountered

7.9 Training and Support

7.9.1 **OmniChat** shall:

(a) Train relevant personnel on handling **Data Subject** requests
(b) Maintain current documentation on procedures
(c) Provide guidance to **Customer** when needed
(d) Update procedures based on experience
(e) Share best practices with **Customer**

7.10 Cost and Fees

7.10.1 **OmniChat** shall:

(a) Provide reasonable assistance at no additional cost
(b) Notify **Customer** if a request requires substantial resources
(c) Agree on any additional fees in advance
(d) Document time and resources spent
(e) Maintain transparent cost structures

8. INTERNATIONAL TRANSFERS

8.1 General Principles

8.1.1 **OmniChat** shall:

(a) **Process Customer Data** primarily within the European Union
(b) Maintain primary infrastructure in specified locations:
- Frontend **Services**: United Kingdom
- Database **Services**: Belgium

(c) Only transfer **Customer Data** outside these locations when:
- Required to provide the **Services**
- Explicitly authorised by **Customer**
- Permitted under applicable **Data Protection Laws**

8.1.2 **AI Model** Processing:

(a) **AI Model** providers may process data in various locations based on their infrastructure
(b) **OmniChat** shall maintain current documentation of **AI Model** processing locations
(c) Customer can request current processing location information for specific models
(d) All **AI Model** providers are bound by appropriate data transfer mechanisms as detailed in Section 8.2

8.2 Transfer Mechanisms

8.2.1 Where international transfers are necessary, **OmniChat** shall ensure at least one of the following mechanisms is in place:

(a) EU Standard Contractual Clauses (SCCs)
(b) UK International Data Transfer Agreement (IDTA)
(c) Binding Corporate Rules
(d) Adequacy decisions issued by relevant authorities
(e) Other valid transfer mechanisms approved under **Data Protection Laws**

8.3 Standard Contractual Clauses

8.3.1 Where applicable, the parties agree that:

(a) The EU SCCs adopted by the European Commission (June 4, 2021) are incorporated by reference
(b) The UK Addendum to the EU SCCs issued by the ICO is incorporated where UK transfers occur
(c) Security measures in Section 5 fulfil the technical and organisational measures required by the SCCs

8.4 SubProcessor Transfers

8.4.1 **OmniChat** shall:

(a) Ensure all **SubProcessors** maintain appropriate transfer mechanisms
(b) Document transfer flows involving **SubProcessors**
(c) Verify **SubProcessor** compliance with transfer requirements

(d) Maintain records of all international transfers
(e) Monitor changes in **SubProcessor** transfer arrangements

8.5 Transfer Impact Assessments

8.5.1 **OmniChat** shall:

(a) Document international transfers, which are limited to API calls to **AI Model** providers and essential cloud infrastructure services
(b) Review transfer arrangements when notified of material changes by **SubProcessors**
(c) Maintain records of data transfer locations and mechanisms
(d) Rely on established safeguards implemented by our cloud and **AI Model** providers
(e) Provide relevant documentation from our **SubProcessors** upon **Customer** request to support their transfer impact assessments

8.6 Additional Safeguards

8.6.1 **OmniChat** shall implement additional safeguards including:

(a) End-to-end encryption for data transfers
(b) Access controls and authentication measures
(c) Data minimisation practices
(d) Regular security assessments
(e) Contractual safeguards with recipients

8.7 Transparency

8.7.1 **OmniChat** shall maintain and provide to **Customer** on request:

(a) Documentation of transfer mechanisms
(b) Lists of countries where data is processed
(c) Details of additional safeguards implemented
(d) Information about relevant legal requirements
(e) Updates on changes to transfer arrangements

8.8 Government Access Requests

8.8.1 If **OmniChat** receives a government access request, it shall:

(a) Notify **Customer** promptly unless legally prohibited
(b) Challenge requests where appropriate
(c) Provide minimum data necessary to comply
(d) Document all requests and responses
(e) Support **Customer** in responding to **Data Subject** inquiries

8.9 Transfer Monitoring

8.9.1 **OmniChat** shall:

(a) Monitor changes in **Data Protection Laws** affecting transfers
(b) Assess impact of legal developments
(c) Update transfer mechanisms as required
(d) Notify **Customer** of relevant changes

(e) Maintain records of monitoring activities

8.10 Suspension of Transfers

8.10.1 **OmniChat** shall:

(a) Suspend transfers if transfer mechanisms become invalid
(b) Notify **Customer** promptly of any suspension
(c) Work with **Customer** to implement alternative arrangements
(d) Document reasons for suspension
(e) Resume transfers only when appropriate safeguards are in place

9. AUDIT & COMPLIANCE

9.1 General Audit Rights

9.1.1 **Customer** shall have the right to audit **OmniChat**'s compliance with this **DPA**, subject to:

(a) Providing reasonable advance notice (minimum 30 days)
(b) Conducting audits no more than once per year
(c) Using mutually agreed independent auditors
(d) Executing appropriate confidentiality agreements
(e) Minimising disruption to **OmniChat**'s operations

9.2 Audit Process

9.2.1 **OmniChat** shall facilitate audits by:

(a) Providing necessary documentation and information
(b) Granting access to relevant personnel
(c) Answering queries in a timely manner
(d) Providing evidence of compliance
(e) Supporting on-site inspections where necessary

9.3 Documentation and Evidence

9.3.1 **OmniChat** shall maintain and make available:

(a) Security policies and procedures
(b) Technical documentation
(c) Training records
(d) Compliance certificates
(e) Audit logs and reports

9.4 Alternative Assurance

9.4.1 **OmniChat** may satisfy audit requirements by providing:

(a) Third-party audit reports
(b) Security certifications
(c) Compliance attestations
(d) Independent assessments

(e) Security questionnaire responses

9.5 Compliance Monitoring

9.5.1 **OmniChat** shall:

(a) Conduct regular internal compliance reviews
(b) Monitor regulatory developments
(c) Update policies and procedures as needed
(d) Track and document compliance activities
(e) Report significant compliance issues to **Customer**

9.6 Audit Findings

9.6.1 Following an audit:

(a) **OmniChat** shall address material findings within agreed timeframes
(b) **Customer** shall provide detailed audit reports
(c) Parties shall agree on remediation plans
(d) **OmniChat** shall provide progress updates
(e) Follow-up audits may be conducted to verify remediation

9.7 Costs and Expenses

9.7.1 Unless otherwise agreed:

(a) Each party bears its own audit costs
(b) **Customer** pays for independent auditor costs
(c) **OmniChat** provides reasonable assistance at no charge
(d) Additional support may incur reasonable fees
(e) Cost arrangements shall be agreed in advance

9.8 Regulatory Investigations

9.8.1 In the event of regulatory investigations, **OmniChat** shall:

(a) Notify **Customer** promptly
(b) Cooperate with investigating authorities
(c) Provide necessary documentation
(d) Coordinate responses with **Customer**
(e) Maintain detailed records

9.9 Continuous Improvement

9.9.1 **OmniChat** shall:

(a) Review audit findings for improvement opportunities
(b) Update security measures based on audit results
(c) Enhance compliance programmes regularly
(d) Share lessons learned with **Customer**
(e) Implement best practices identified during audits

9.10 Reporting

9.10.1 **OmniChat** shall provide:

(a) Regular compliance status updates
(b) Incident reports when required
(c) Audit summary reports
(d) Remediation progress reports
(e) Annual compliance certificates

10. TERM & TERMINATION

10.1 Term

10.1.1 This **DPA** shall:

(a) Come into effect on the date of the **Agreement**
(b) Remain in effect for the duration of the **Agreement**
(c) Continue to apply to any **Customer Data** retained after termination
(d) Survive termination for provisions that by their nature should survive
(e) Be coterminous with the **Agreement** unless otherwise specified

10.2 Termination Events

10.2.1 This **DPA** may be terminated:

(a) Automatically upon termination of the **Agreement**
(b) By **Customer** if **OmniChat** breaches any material term of this **DPA**
(c) By either party if continued performance becomes illegal
(d) As otherwise provided in the **Agreement**
(e) By mutual written agreement of the parties

10.3 Data Export and Return

10.3.1 **Customer** shall:

(a) Be responsible for exporting their data prior to termination using **OmniChat**'s self-service export features as described in Section 7.5
(b) Maintain their own copies of exported data
(c) Complete any desired exports before the termination date

10.3.2 **OmniChat** shall:

(a) Maintain the export functionality until the termination date
(b) Provide documentation on how to use export features
(c) Ensure export features remain operational during termination period
(d) Provide reasonable technical support if export issues arise

10.4 Data Deletion

10.4.1 Following termination:

(a) **Customer** access to the **Services** will cease

(b) **OmniChat** shall permanently delete all **Customer Data** within 30 days
(c) Deletion shall include all copies in production systems and backups
(d) **SubProcessors** shall be instructed to delete **Customer Data**
(e) Written confirmation of deletion will be provided upon request

10.5 Retention Requirements

10.5.1 OmniChat may retain Customer Data:

(a) As required by applicable law
(b) For defending legal claims
(c) In anonymised form for analytical purposes
(d) As explicitly authorised by **Customer**
(e) As necessary to protect **OmniChat**'s legal rights

10.6 Transition Assistance

10.6.1 **OmniChat** shall provide reasonable assistance to:

(a) Facilitate smooth transition to another provider
(b) Ensure continuity of service
(c) Transfer **Customer Data** securely
(d) Document transition processes
(e) Support **Customer**'s exit planning

10.7 Costs

10.7.1 Unless otherwise agreed:

(a) Standard data export and deletion is provided at no cost
(b) Custom formats or expedited **Services** may incur reasonable fees
(c) Extended transition support may be subject to additional charges
(d) Cost estimates shall be provided in advance
(e) Payment terms shall follow the **Agreement**

10.8 Surviving Obligations

10.8.1 The following obligations shall survive termination:

(a) Confidentiality obligations
(b) Data protection obligations
(c) Security breach notification requirements
(d) Audit rights for retained data
(e) Indemnification provisions

10.9 Documentation

10.9.1 **OmniChat** shall maintain records of:

(a) Termination events and dates
(b) Data return activities
(c) Deletion certificates
(d) Retention justifications

(e) Transition assistance provided

10.10 Final Certification

10.10.1 Upon completion of all post-termination obligations, **OmniChat** shall:

(a) Provide final written certification of compliance
(b) Confirm completion of all data-related obligations
(c) Document any retained data and justification
(d) Return or destroy any remaining confidential information
(e) Maintain records as required by law

11. LIMITATION OF LIABILITY

11.1 Liability Cap

Provider's liability under this DPA shall be subject to the limitations of liability set forth in the main Agreement. The aggregate liability of **Provider** for all claims arising under this DPA shall not exceed the total fees paid by **Customer** during the thirteen (13) month period preceding the event giving rise to the claim.

11.2 Exceptions

The limitation in Section 11.1 shall not apply to:
(a) **Provider's** gross negligence, fraud, or wilful misconduct attributable to **Provider's** own acts or omissions (and not those of its **SubProcessors** where **Provider** has fulfilled its due diligence, contracting, and monitoring obligations under Section 6); or
(b) Death or personal injury caused by **Provider's** negligence.

11.3 SubProcessor Claims

For the avoidance of doubt, claims arising from the acts or omissions of **SubProcessors** shall remain subject to the limitation of liability set forth in Section 11.1, provided that **Provider** has fulfilled its due diligence, contracting, and monitoring obligations under Section 6.

11.4 Regulatory Fines

Where a Supervisory Authority imposes a fine or penalty directly on **Customer** as a result of **Provider's** material breach of this DPA, **Provider** shall indemnify **Customer** for such fine or penalty, subject to:
(a) the aggregate cap set forth in Section 11.1;
(b) **Customer** providing prompt written notice of the fine or penalty;
(c) **Customer** providing **Provider** reasonable opportunity to engage with the Supervisory Authority (where permitted by law); and
(d) the fine or penalty not arising from **Customer's** own acts, omissions, or instructions.