Schedule 1 – Data Processing Agreement.

Definitions

Controller, Data Subject, Personal Data, Processor, Sub-Processor, Data Protection Impact Assessment, Data Subject Access Request have the same meaning as in the UK GDPR.

1 Where the Parties are Independent Controllers of Personal Data

1.1 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

1.2 Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

1.3 The Parties shall only provide Personal Data to each other:

1.3.1 to the extent necessary to perform the respective obligations under this Agreement;
1.3.2 in compliance with the Data Protection Legislation (including by ensuring all required fair Processing information has been given to affected Data Subjects);

1.4 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

1.5 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under this Agreement.

2. The Customer as a Controller and C360 as Processor

2.1 The Controller shall be responsible, among other, for ensuring that the Processing of Personal Data, which the Processor is instructed to perform, has a legal basis.

2.2 The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be agreed in writing and documented.

2.3 On termination of the provision of personal data processing services, the data processor shall be under obligation to delete or put beyond use all personal data processed on behalf of the data controller and confirm to the data controller that it has done so unless the law or the Agreement requires storage of the personal data.

2.4 The parties may contact each other using the following contacts/contact points:

The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

Personal data is processed for the following purposes:

Service Provision - To provide and operate the voice and chat platform. To deliver AI agent services (e.g. answering questions, executing tasks, etc.). To enable user interactions via voice or text.
Authentication and Security - To verify user identities, Access control, and fraud prevention
Security and Fraud prevention – To detect and respond to suspicious or harmful activity; to secure the platform from misuse or attacks.
Personalisation and Contextual Responses - To tailor conversations based on user history, preferences, or location. To improve contextual accuracy of AI agent responses.
Communication and Notifications – To send alerts, reminders or confirmations, to follow up on conversations.
Analytics and Optimization - Usage tracking, performance optimization, and service improvement
Marketing and Attribution - To send users updates, promotions, or feature announcements. To conduct surveys or gather user feedback.
Legal Compliance - Meeting legal obligations and regulatory requirements
Customer Support - To resolve user issues and provide assistance. To review past interactions to improve support efficiency.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

To fulfil the delivery of the Services.

A.3. The processing includes the following types of personal data about data subjects:

Contact Information – names, email addresses, phone numbers, user ID or account ID, organisation name
Voice and Audio Data – Speech to text and messaging transcripts.
Chat and Interaction Data - Chat transcripts, Message content (text inputs, intents, responses),
Interaction history, Commands, queries, and natural language inputs, Conversation metadata (timestamps, session ID, agent/user involved)
Technical Data - IP addresses, device type and operating system, Browser type/version,
Connection and session logs, Location data (e.g. inferred from IP), Usage patterns (e.g. frequency, duration, behaviour analytics)
Authentication and Access Data - Used to verify identity and control access to features or accounts, Login credentials (hashed passwords).
Support and Feedback Data - support queries, Survey responses, Feedback or satisfaction ratings, Uploaded files or screenshots.
Usage and Analytics Data - credits and usage tracking, file storage usage statistics, system analytics and metrics.
Cookies and Tracking Data - Session cookies, analytics cookies (website only), preference cookies.
Log Data - Technical system logs, access logs, error logs

A.4. Processing includes the following categories of data subject:

Employees, Authorised Users and End Users of C360 Customers.

A.5. Duration of the data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

Term of the Agreement.

Appendix B Third Party Tool

B.1. Approved Third Party Tools

The data controller authorises the engagement of the following third party tools:

Service	Company	Purpose
Amazon Web Services	AWS Region Europe (London) AWS eu-West-1 (Ireland)	To host and run application servers, AI models, speech models, and APIs that power the voice/chat platform
Google Gemini (and successor models)	Europe-west2 region (London)	Text-to-Speech, Speech-to-Text, dialog generation, and audio/dialog rendering services as part of the voice agent function
Pinecone	GCP EU-West-1 (Ireland)	Vector Databases

The data controller authorises the engagement of the following sub-processors:

Company	Purpose
Voximplant	Voice/Chat/SMS services
Twilio	Voice/Chat/SMS services

The data controller shall on the commencement of the Agreement authorise the use of the abovementioned third party tools for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a third party tool for a 'different' processing than the one which has been agreed upon or have another third party tool perform the described processing.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out in order to deliver the Services.

C.2. Security of processing

The level of security shall take into account:

The data processor shall make decisions about the technical and organisational security measures that are to be applied to create the necessary level of data security.

The data processor shall – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

- Measures of encryption of personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Processes for assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
- Measures for role based access control
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which personal data are processed
- Measures for logging and monitoring
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for ensuring data minimisation
- Measures for ensuring data quality
- Measures for honouring data retention rules.
- Measures for ensuring accountability
- Measures for allowing data portability and ensuring erasure

C.3. Assistance to the data controller

The data processor shall, at the data controllers expense, assist with Data Subject Access Requests, Data Protection Impact Assessments and liaising with the Information Commissioners Office as necessary.

C.4. Storage period/erasure procedures

Chat Messages and Conversations - Retained by the maximum retention period of the user's plan or shorter upon user's requirement
Lead Data - Retained as long as the chatbot is kept
User Account Data - Retained while account is active plus 30 days after deletion request
Log Data - Retained for maximum of 30 days.
Session Cookies – Session cookies not used.
Analytics Cookies – Analytics cookies not used.

C.5. Processing location

Processing of the personal data under the Agreement cannot be performed at locations outside the UK unless it is in accordance with UK GDPR transfer mechanisms.

C.6. Procedures for the data controller’s audits of the processing of personal data being performed by the data processor

The data processor shall maintain complete and accurate records and information to demonstrate its compliance with the UK GDPR and allow for audits by the Customer or the Customer's designated auditor and immediately inform the Customer if, in the opinion of the Provider, an instruction infringes the Data Protection Legislation.