

Terms of use

Version 1.2 · in force since 27/10/2026

Document id: hogrh0t9s64gccc9x08wsazo · issued on 27/10/2026

PREAMBLE

The company Manifone, a simplified joint-stock company with a share capital of 100,000.00 euros, registered with the Vannes Trade and Companies Register under number 492 486 014, whose registered office is located at 10, rue Henri Becquerel, PIBS, 56000 Vannes (hereinafter the "Provider"), publishes and operates, under the trade name " Manivox ", a software platform accessible in SaaS mode allowing the creation, deployment and supervision of voice conversational agents based on artificial intelligence (hereinafter the "Platform"). The Provider is also a declared electronic communications operator and provides, as part of the Service, the numbers and lines necessary for the operation of the Agents.

The Platform is intended to be subscribed to by professionals who use it for their own needs or, as Distributors or integrators, for the needs of their own clients, within the framework of deploying customer relationship, support, appointment scheduling, prospecting solutions or any other use case involving a voice conversational agent. The Client markets the Service either under the Manivox brand, or under its own brand, under the conditions of Article 15 bis.

These general terms of use (hereinafter the "General Terms" or "GTU") are intended to define the conditions under which the Provider makes the Platform available to the Client, as well as the respective rights and obligations of the Parties in the context of this provision.

The elements specific to each Client, and in particular the identification of the Parties, the Brand Regime and, where applicable, the agreed retention periods, the initial duration and the effective date of the Contract, are recorded in the Order. The processing of personal data carried out by the Provider on behalf of the Client is governed by the DPA, a separate document accessible by link from the Console and from these presents, acceptance of which results from acceptance of the Order. The configuration and parameterization services for the Agents that the Provider may perform on behalf of the Client are subject to a separate service contract, to which the DPA remains applicable.

The Client acknowledges having read these General Terms and Conditions and the DPA prior to accepting them and declares that they have the competence and necessary means to subscribe to the Platform and to use it in accordance with its intended purpose.

1. DEFINITIONS

The following terms and expressions, when used with an initial capital letter, have the meaning assigned to them in this article. The defined terms are used interchangeably in the singular or plural as appropriate to the context.

"Agent": means the conversational software component operated by the Provider within the Platform, configured and set up by the Client according to its use cases, which orchestrates calls to the LLM and external tools, applies the Client's Prompts, implements the RAG, and generates voice Outputs for End Users.

"Audio": means the audio signal corresponding to Conversations between End Users and Agents, captured by the Platform and which may be recorded, transcribed, processed, and stored under the conditions defined herein.

"Outbound Campaign": means any series of calls made by one or more Agents at the Client's initiative to a list of recipients, notably for commercial prospecting, follow-up, or notification purposes.

"API Key": means the authentication key allowing access to a third-party service, notably to an LLM or a connector, provided by the Client as part of the BYOK option.

"Client": means the legal entity that has accepted an Order and these General Terms and Conditions, which subscribes to the Service. The Client acts as a professional, whether using the Platform for its own needs or as a distributor or integrator for the needs of its Underlying Clients. The Client is referred to as "Distributor" in the DPA.

"Underlying Client": means any professional client of the Client on whose behalf the latter configures or operates one or more Agents by means of the Platform, as part of the service it provides to it, whether or not that client accesses the Platform or the Client Portal under the conditions set out in Article 8. The Underlying Client is referred to as "End Client" in the DPA.

"Order": means the order form, subscription document, or subscription summary, in written or electronic form, accepted by the Client, which identifies the Parties, the Brand Regime, the initial term, and the effective date of the Contract, and refers for the remainder to these General Terms and Conditions, the DPA, and their annexes. The Order only derogates from these General Terms and Conditions to the strict extent that it expressly so provides.

"Console": means the management and supervision interface made available to the Client by the Provider, allowing in particular the configuration of Agents, consultation of Conversations, their transcriptions, associated Prompts and generated Outputs, as well as monitoring of usage and performance indicators. The Client Portal is the view of this interface open to Underlying Clients.

"Contract": means the whole formed by the Order, these General Terms and Conditions, the DPA and their appendices. The Contract is referred to as the "Framework Contract" in the DPA.

"Conversation": means any voice exchange between an End User and an Agent transiting through the Platform, including the captured Audio, its transcription, the associated Prompts and Outputs, and the resulting indicators.

« **Copilot** » : means the optional function for assisting in the design of Agents, available as standard and involving the transmission of content only in the event of actual use, based on a third-party language model identified in the DPA and in the Register of Processors. "KB Doctor" means the function for analyzing knowledge bases based on a model self-hosted by the Provider.

"Client Data": means all data, content, settings, Prompts, knowledge bases, files and information transmitted or made accessible by the Client or its Authorized Users to the Provider, excluding the Provider's proprietary elements.

"DPA": means the data processing agreement concluded between the Parties in accordance with Article 28 of Regulation (EU) 2016/679, which governs the processing of personal data that the Platform necessarily requires the Provider to carry out on behalf of the Client. The DPA is accessible via a link from the Console and from these terms; its acceptance results from acceptance of the Order.

"Business Hours": refer to the time slots from Monday to Friday from 9:00 to 18:00, Paris time, excluding legal public holidays in France.

"Credentials": means all authentication elements (username, password, second factor, access key) allowing an Authorized User to access the Platform.

"LLM": means the language model used by the Agents to generate their Outputs. Unless the Client uses the BYOK option, the LLM is a self-hosted model by the Provider on its infrastructure; the Provider does not supply any third-party LLM under its own contract for the conversational processing of the Agents.

« **Manivox** » : means the trade name under which the Provider operates its voice conversational agent business and, depending on the context, the Platform itself. Manivox is not a separate legal entity from the Provider.

"Brand": means the " Manivox" brand, the associated logos and distinctive signs, of which the Provider is the holder.

"Numbers": means the telephone numbers and call lines assigned by the Provider, in its capacity as an electronic communications operator, to the Underlying Client on whose behalf the Agents are operated or, where the Agents are operated for the Client's own needs, to the Client, enabling End Users to connect with the Agents and Agents to make calls.

"BYOK Option": or "Bring Your Own Key": means the option offered to the Client, under the conditions defined in Article 5, to provide its own API Key or its own access so that the Agents can call upon an LLM, a knowledge base, a chatbot, a web service, an MCP server, or any other third-party tool

provided directly by the Client from its own provider.

"Client Storage Option": means the option, implemented by configuring the Client's account in the Console, by which the Audio is directly stored on the object storage infrastructure designated by the Client, under the conditions of Article 6.1.

"Output": means any result generated by the Agents in response to a Conversation, including in particular the textual responses produced by the LLM, their voice rendering, transcriptions, summaries, and any resulting indicator.

"Platform": means the SaaS software solution published and operated by the Provider under the Manivox brand, including in particular the agent orchestration engine, the audio pipeline (capture, transcription, generation, rendering), the RAG, the Console, the Client Portal, as well as the features described in Article 4.

"Client Portal": means the view of the Console, hosted on the manivox.ai domain, to which the Client may grant access to Authorized Users of its Underlying Clients to consult the data of their own account only, under the conditions of Article 8.

"Prompt": means any instruction, guideline, directive, or rule configured by the Client or its Authorized Users in order to define the behavior, scope, and usage rules of the Agents. The Prompts constitute a proprietary asset of the Client.

"RAG": or " Retrieval-Augmented Generation ": means the Provider's proprietary mechanism allowing the Agents to enrich their Outputs from the knowledge bases created by the Client.

"Brand Regime": means the method of marketing the Service chosen by the Client in the Order in accordance with Article 15 bis: under the Brand (Option 1) or as White Label (Option 2). "White Label" means the marketing of the Service by the Client under its own brand, within the limits of Article 15 bis.

"AI Regulation": means Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, as well as its implementing texts and any regulatory developments supplementing or replacing it.

"Service": means all services provided by the Provider to the Client under the Contract, including in particular access to the Platform, its features, the Numbers, and associated support.

"Register of Processors": means the up-to-date version of the DPA annex listing sub-processors, maintained by the Provider in the Legal area of the Console and accessible to the Client after authentication, as well as, for consultation, in the form of a neutral list, to Authorized Users of the Client Portal. It constitutes the authoritative register of sub-processors involved for the Platform and indicates the location of their processing and the identity of the self-hosted models in use. It is not public.

“Authorized User”: means any natural person to whom the Client grants Credentials, whether a collaborator of the Client, a provider acting on its behalf, a collaborator of an Underlying Client, or any other person authorized by the Client to access the Platform or the Client Portal.

“End User”: means the natural person who interacts with an Agent in the context of a Conversation. The End User is not a party to the Contract.

1 bis. CORRESPONDENCE WITH THE TERMS OF THE DPA

These General Terms describe the commercial relationship between the Parties; the DPA describes the processing of personal data. Both documents sometimes refer to the same realities by different terms. The table in Annex B sets out the applicable correspondences. In case of doubt regarding a data protection issue, the definition in the DPA prevails; for any other issue, that of these General Terms prevails.

2. CONTRACTUAL DOCUMENTS AND HIERARCHY

The Contract is composed of the Order, these General Terms, the DPA, and their annexes.

In the event of any conflict between these documents, the Order prevails over the General Terms and Conditions, which in turn prevail over their appendices. The DPA prevails over all other contractual documents exclusively with regard to matters relating to the processing of personal data; for any other matter, these present terms prevail over the DPA.

The technical and functional documentation of the Platform accessible from the Console or communicated by the Provider to the Client is for informational purposes and does not constitute a contractual document, unless expressly stated otherwise.

3. ACCEPTANCE OF THE GENERAL TERMS AND CONDITIONS AND ACCESS TO THE PLATFORM

3.1 Acceptance

Acceptance of these General Terms and Conditions results from the acceptance of the Order by a person duly authorized to bind the Client. Prior to this acceptance, the General Terms and Conditions and the DPA are brought to the Client's attention and remain accessible to them at any time on the Platform, with an indication of their version and date. Acceptance of the Order constitutes the Client's adherence to these present terms and to the DPA, both for themselves and for all their Authorized Users, for whom the Client guarantees compliance with these present terms under the conditions of Article 8. The Client may also generate at any time, from the Console, a confirmation copy of the DPA intended to be signed by both Parties; this signature does not condition either the conclusion or the

enforceability of the DPA, which is acquired by adherence.

Any modification of the General Terms and Conditions is brought to the Client's attention and becomes enforceable against them under the conditions provided for in Article 19.

3.2 Creation of the account and first access

The Provider opens a dedicated account for the Client on the Platform within a reasonable period from the acceptance of the Order. The Provider communicates to the Client the Identifiers necessary for initial access to the Console, and the Client is responsible for changing them upon first login and keeping them secure.

3.3 Technical prerequisites

Access to the Platform requires that the Client has a technical environment allowing the use of the Service under normal conditions, in particular suitable Internet connectivity and, where applicable, a telephone infrastructure compatible with the Platform's flows. The Client is solely responsible for providing this environment and for the related costs.

4. DESCRIPTION OF THE SERVICE

4.1 Functional scope

The Platform provides the Client, its Authorized Users and, where applicable, its Underlying Clients, with the following functionalities:

- the creation, configuration and deployment of voice conversational Agents capable of interacting in natural language with End Users, including version management and comparative testing;
- the provision of an audio pipeline including voice capture, real-time transcription by a speech recognition engine ("speech-to-text" or "STT"), generation of Outputs by calling an LLM, and voice rendering by a text-to-speech engine ("text-to-speech" or "TTS");
- the configuration of Prompts allowing the definition of the behavior, tone, scope and limits of the Agents;
- the RAG, powered by uploaded documents, web pages indexed at the Client's request or sources connected by the Client;
- the connection to third-party tools (notably customer relationship management systems, calendars, business information systems) via connectors integrated into the Platform or web services configured by the Client, subject to the specific conditions of these third-party tools;
- the Console allowing supervision of Conversations, listening to Audio within the limit of its retention period, consultation of transcriptions, Prompts and associated Outputs, monitoring of usage and

performance indicators, generation of summaries and reports, as well as the Client Portal open to Underlying Clients under the conditions of Article 8;

- the optional artificial intelligence assistance functions Copilot and KB Doctor;
- the Outbound Campaigns, with configuration of time slots, cadence and new call attempts, under the conditions of Article 4 bis;
- interconnection, by trunk SIP, of the Client's or its Underlying Clients' telephony infrastructure, under the conditions of Article 4 bis.

The use of the Platform requires the use of one or more Numbers provided by the Provider under the conditions of Article 4 bis. The provision, assignment and invoicing of the Numbers may be subject to specific conditions specified in the Order, on the Platform and in Annex D and may give rise to separate remuneration from the main Service.

The precise technical and functional characteristics of the Platform are described in the documentation accessible from the Console and may evolve under the conditions set out in Article 4.2 below.

4.2 Service Evolution

The Platform is scalable. The Provider may, at any time, change the functional scope of the Service, in particular by adding new features, modifying existing features, or removing certain features, notably for technical, security, compliance, end of support, obsolescence reasons, or due to constraints imposed by its own suppliers.

The Provider informs the Client of these changes by any appropriate means, including by notification from the Console. When a change is likely to substantially and adversely affect the Client's use of the Platform, it is notified to the Client in writing with reasonable prior notice. If such a change results in a material degradation of the Service, the Client has the right to terminate the Contract without penalty under the conditions set out in Article 18.

4 bis. ELECTRONIC COMMUNICATIONS SERVICES

4 bis.1 Operator Status and Numbers

The Provider is a declared electronic communications operator with the Regulatory Authority for Electronic Communications, Postal Services and Print Media Distribution (ARCEP) or the equivalent authority of the relevant country. It assigns the Numbers necessary for the operation of the Agents to the Underlying Client on whose behalf they are operated, which thereby becomes their assignee within the meaning of the national numbering plan, or to the Client where the Agents are operated for its own needs, under the conditions of the Order and, for Underlying Clients, of the mandate provided for below, in compliance with the applicable numbering plan and the rules for allocation, use, and return of numbering resources. The Numbers remain public resources of which neither the Client nor the

Underlying Client acquires ownership; they are used in accordance with their intended purpose and, upon termination of the Contract or of the assignment, are returned or, at the request of their assignee, ported under regulatory conditions.

In this capacity, the Provider is subject to its own legal obligations, in particular the retention of certain traffic data and responding to requests from competent authorities, which it carries out independently of the Client's instructions and the retention periods provided for in the Contract, as specified in the DPA.

The Numbers assigned to an Underlying Client are ordered, terminated and configured by the Client as agent of that Underlying Client, under a Numbers management mandate drawn up in accordance with the template made available in the Console and signed electronically by the Underlying Client, from the Console, prior to any order. The Client may not delete or modify the essential provisions of the mandate listed in Annex D. It warrants the accuracy of the identification and notification details of the Underlying Client that it enters therein and reports any change without delay. It warrants that the person it invites to sign the mandate is authorized to bind the Underlying Client and that the signature email address entered is accurate and personal to that person. Upon termination of the contract binding it to an Underlying Client, the Client shall, without delay and from the Console, terminate the Numbers assigned to that Underlying Client, unless a porting request is made by the Underlying Client. The Provider is not a party to the mandate, certain provisions of which are nevertheless stipulated for its benefit (Annex D). The Numbers are invoiced to the Client under the conditions of Article 10; their re-invoicing to the Underlying Client falls solely within the contract binding them.

4 bis.2 Interconnection by trunk SIP

When the Client or its Downstream Client connects its own telephony infrastructure to the Provider's network by trunk SIP, it remains solely responsible for its network, its equipment, its own operator or user obligations, and the security of its infrastructure up to the interconnection point with the Provider's network. Authentication of the trunk is based on the source IP addresses declared by the Client, who guarantees their accuracy and updating. The Client shall give preference to SIP transport over TLS with media encryption; unencrypted transport remains under its sole responsibility. Unavailabilities attributable to the connected infrastructure are excluded from the service level commitments.

4 bis.3 Outbound Campaigns

The Client is solely responsible for the lawfulness of any Outbound Campaign that it configures or allows its Downstream Clients to configure. It acknowledges that, since 11 August 2026, any commercial prospecting call to a consumer in France is subject to a prior consent regime (Article L223-1 of the Consumer Code, as amended by Law No. 2025-594 of 30 June 2025 and its implementing decree), that the rules relating to authorized days, times and frequencies of prospecting and to caller

identification remain applicable, and that different regimes may apply in other countries and to business-to-business prospecting.

- Before launching any Outbound Campaign for commercial prospecting purposes, the Client certifies, by means of the checkbox provided for this purpose on the Platform, that the called numbers are subject to prior consent in accordance with the applicable regulations and that the campaign complies with the rules on times and frequency. This certification, timestamped and retained by the Provider, does not constitute proof of the consent of the called persons, which the Client alone is required to collect, retain for the legal duration, and produce upon any request from the Provider or an authority;
- The Client configures the time slots, the rate, and the new call attempts in accordance with the applicable regulations;
- The Provider may suspend an ongoing Outbound Campaign in the event of reasonable doubt, report, complaint, or request from an authority, without such suspension giving rise to any right to compensation;
- Any inaccurate certification engages the sole responsibility of the Client, who shall indemnify the Provider under the conditions of Article 9.3.

5. CONNECTIVITY TO THE LLM AND THIRD-PARTY TOOLS

5.1 Default regime: self-hosted LLM

Unless the Client uses the BYOK option, the Agents use a self-hosted LLM by the Provider on its own infrastructure located in France, without transmission of Conversations to a third-party model provider. The Provider selects, at its discretion, the self-hosted model(s) made available to the Platform and is free to change the choice in order to optimize the quality, performance, security, compliance, or costs of the Service; the identity of the current model is indicated in the Register of Processors for information purposes. The Client does not control the choice of model in this regime. The Provider does not supply any third-party LLM under its own contract for the conversational processing of the Agents; the list of technically validated third-party models published in the documentation does not constitute either a recommendation or a contractual relationship between the Provider and these suppliers.

The performance and availability of the LLM thus provided are ensured by the Provider within the framework of the service level commitments set out in Annex A and within the inherent limitations of generative artificial intelligence models as recalled in Article 14.

5.2 BYOK Option

The Client may, when this option is offered by the Provider, choose to provide its own API Key or its own access allowing the Agents to call upon an LLM, an external knowledge base, a chatbot, a web service, an MCP server or any other third-party tool the provision of which is ensured directly by the Client with its own provider. The provisions of this article apply to each of these third parties.

In this case:

- the Client is solely responsible for the selection of the third party, the subscription with its provider, compliance with the terms of use imposed by the latter, the securing of the API Key and the payment of amounts due to its provider;
- the LLM constitutes a technical prerequisite for the operation of the Service; in the event of unavailability of the Client's LLM or failure of the API Key, the Platform cannot produce Outputs and the Provider cannot be held liable therefor;
- the performance, availability, quality, accuracy and regulatory compliance of the responses of the Client's LLM and third-party tools are not guaranteed by the Provider and any failure of these third parties is excluded from the service level commitments set out in Annex A;
- the Client's API Key is stored by the Provider in its secret management system, encrypted in accordance with the state of the art; the Client is responsible for rotating its API Key in case of suspected compromise;
- the Client guarantees that, with each third party processing personal data on its behalf, it has a data processing agreement compliant with the GDPR and informs the Provider, upon the first connection of each new third party, by means of the declaration provided for this purpose in the Console; these third parties are not sub-processors of the Provider.

The Provider may make the implementation of the BYOK option subject to prior technical verification of the compatibility of the third party chosen by the Client with the Platform. The Provider may refuse or suspend the implementation of BYOK with a third party that presents a technical, contractual or regulatory incompatibility, a security risk or behavior likely to affect the proper functioning of the Platform or the quality of the Service.

6. HOSTING, LOCATION AND RETENTION OF DATA

6.1 Hosting of the Platform and Client Storage Option

The Provider ensures the hosting of the core of the Platform (orchestration, telephony, databases, RAG, self-hosted models, main speech synthesis, Console and Client Portal) in France, on its own infrastructure and by means of its hosting provider(s), identified in the DPA and the Register of Processors. Certain components of the audio pipeline and certain optional functions use third-party processors, whose list, location and transfer conditions are kept up to date in the Register of

Processors and governed by the DPA.

When the Client implements this option by configuring its account in the Console, the Audio may be directly stored on the object storage infrastructure designated by the Client (Client Storage Option).

In this configuration:

- the Client guarantees the availability, security and compliance of its storage infrastructure, the location and regulatory compliance of which are its sole responsibility;
- the Provider's service level commitments do not apply to the portion of the storage infrastructure under the Client's responsibility;
- the Provider cannot be held liable for any loss, alteration or unavailability of the Audio resulting from a failure of the Client's storage infrastructure;
- the Client provides the Provider with all configuration information and access necessary for the proper functioning of this integration and keeps this information up to date;
- the Provider does not retain any permanent copy of the Audio thus stored; the retention period, deletion and processing of End Users' requests relating to this Audio are the sole responsibility of the Client, as specified in the DPA.

6.2 Storage and retention of Audio

When the recording of Audio is enabled for the Client's account and outside the Client Storage Option, the Provider retains the Audio in a dedicated storage space hosted in France for a maximum period of one (1) week from the end of the Conversation, unless a different period is specified in the Order within the maximum period authorized by the Provider. Upon expiry of this period, the Audio is irreversibly deleted.

The Client may, under the technical conditions provided by the Platform, export the Audio within the limit of its retention period. Beyond this, the Audio is no longer accessible and cannot be restored.

6.3 Storage and retention of transcriptions and indicators

The transcriptions of Conversations, associated Prompts, textual Outputs, summaries, tool call logs, and usage and performance indicators are retained in a dedicated Provider database for the duration specified in the Order. The Client may, under the technical conditions provided by the Platform, configure the retention period of these elements within the limits defined by the Provider.

7. ACCEPTABLE USE CONDITIONS

7.1 General principle

The Client undertakes to use the Platform in accordance with its intended purpose, in compliance with these General Conditions, the Order, the DPA, the Platform documentation, and the applicable regulations. The Client guarantees that its Authorized Users and its Underlying Clients comply with the same commitments.

7.2 Prohibited uses

The Client is prohibited, and prohibits its Authorized Users and its Underlying Clients from:

- using the Platform for unlawful, fraudulent purposes, contrary to public order, or facilitating the commission of an offense;
- using the Platform in use cases prohibited by the AI Regulation, notably those covered by Article 5 of said regulation, including subliminal techniques, exploitation of vulnerabilities, social scoring, or emotion recognition in the workplace or in educational establishments;
- to configure, or allow an Underlying Client to configure, an Agent falling under high-risk artificial intelligence systems referred to in Annex III of the AI Regulation — notably the evaluation and sorting of emergency calls, recruitment and management of workers, creditworthiness assessment, or access to essential public or private services — without the prior written consent of the Provider, who may make it subject to contractual adjustments or refuse it;
- to configure an Agent with the aim of misleading End Users about the artificial nature of their interlocutor, or to configure an Agent intended to impersonate an identified or identifiable natural person without that person's consent;
- using the synthetic voice generated by the Platform to produce audio " deepfake " content without clear prior information to the recipients;
- using the Platform for commercial prospecting purposes in violation of Article L223-1 of the Consumer Code (prior consent of the consumer), rules relating to days, times, and frequencies of prospecting, the Postal and Electronic Communications Code, or any other applicable regulation regarding prospecting, in France or in any other destination country of the calls;
- of to disable, bypass or alter the transparency and marking mechanisms for content generated by artificial intelligence made available by the Platform;
- to inject into the Platform Prompts or Client Data intended to divert the Platform from its purpose, to bypass its control mechanisms or to obtain Outputs unrelated to the subscribed functionalities;
- to introduce into the Platform any malicious code, virus, worm, Trojan horse or element likely to compromise its integrity, security or proper functioning, to attempt unauthorized access to the Platform, its components or other clients' data, or to subject the Platform to abnormal loads, unauthorized penetration tests, probing, scanning or vulnerability analysis operations;
- to use the Platform in a way that artificially generates Conversations with the aim of distorting indicators or billing, saturating the Service or deriving undue advantage from it;

- to share Identifiers among several natural persons;
- to use the Platform in a use case contrary to the terms of use imposed by the providers of third-party tools used by the Client as part of the BYOK option.

7.3 Measures in case of non-compliant use

In the event of a breach of Article 7, the Provider reserves the right, after notification to the Client, to take any measure proportionate to the breaches observed, including restricting, suspending or terminating access to the Platform under the conditions set out in Article 18.

When the seriousness of the facts or urgency so justifies, particularly in the event of a breach of security or the rights of third parties, these measures may be taken without prior notice.

7.4 Fraud and abnormal use detection

The Provider implements automated systems to detect abnormal or fraudulent behavior likely to affect the security, availability or financial integrity of the Service. The Client is required to cooperate in good faith with the Provider in the event of an investigation concerning suspicious use of its account and remains responsible for amounts invoiced resulting from any use of the Client's account, unless it demonstrates a fault on the part of the Provider.

8. AUTHORIZED USERS AND UNDERLYING CLIENTS

8.1 Granting access

The Client may grant Identifiers to the Platform to natural persons of its choice, within the limit provided in the Order where applicable. Any natural person receiving Identifiers becomes an Authorized User within the meaning of the Contract.

The Client is solely responsible for granting, managing, and revoking access for its Authorized Users. The Client guarantees that these Authorized Users comply with these General Terms and Conditions and, in particular, the acceptable use conditions set out in Article 7. The Client is liable, as for its own actions, for any act, omission, or breach by its Authorized Users in connection with their use of the Platform.

8.2 Underlying Clients

The Client may, as part of the service it provides to its own professional clients, configure and operate Agents on their behalf. The following cumulative conditions apply to each Underlying Client, whether or not it has access to the Client Portal or to an interface developed by the Client:

- the Underlying Client acts exclusively in a professional capacity;
- the Client contractually requires the Underlying Client to comply with provisions reflecting, in substance, the contractual baseline set out in Annex C, as well as with obligations equivalent to those arising from these General Terms and Conditions and the DPA, in particular regarding acceptable use conditions, protection of personal data (the Underlying Client being, in general, the controller of the End Users' data), intellectual property, confidentiality, and compliance with the AI Regulation;
- subject to the assignment of the Numbers to the Underlying Client under the mandate provided for in Article 4 bis.1, the Client remains the sole contracting party of the Provider and remains fully liable, towards the Provider, for any act, omission, or breach by the Underlying Client and its own users as if they were acts or breaches of the Client;
- the Client may not operate an Agent on behalf of an Underlying Client, nor grant it access to the Platform, where that Underlying Client carries out an activity competing with that of the Provider or would use the Platform to develop a competing product or service.

8.3 Client Portal

The Client may allow its Underlying Clients to access the Client Portal and use its features, in compliance with the conditions of Article 8.2. Access to the Client Portal is optional and is not a condition for operating Agents on behalf of an Underlying Client.

The Client Portal is accessible in read-only mode, except for actions reserved for its administrators (user management; direct entry, update, and refresh, by the Underlying Client, of its login credentials for third-party tools — as an alternative to entry by the Client — solely within the framework of the Connectors made available by the Client and without direct access to the integration platform). It provides, for consultation, access to the Register of Processors in the form of a neutral list. The Client determines, for each Underlying Client, the visible sections and roles. The Client Portal's 'as account' preview function, accessible to the Client from the Console, constitutes access to the data of the relevant Underlying Client; the Client uses it only for support and verification purposes, informs the Underlying Client, and acknowledges that such access is logged.

The Provider may, in the event of a proven risk to the security, integrity of the Platform or the rights of third parties, refuse or revoke access of an identified Underlying Client, after informing the Client.

8.4 Access Security

The Client implements appropriate measures to ensure the security of the Credentials of its Authorized Users, including:

- to keep the Credentials confidential and ensure that they are not shared between several natural persons;
- to activate, when the Platform offers it, multi-factor authentication for privileged accounts;
- to implement an access management policy based on the principle of least privilege;
- to revoke without delay the access of Authorized Users who are no longer authorized to use the Platform, in particular in the event of departure or change of functions;
- to issue and renew in a secure manner the Credentials of the Authorized Users of the Client Portal, whose password cannot be reset in self-service;
- to notify without delay the Provider of any compromise or suspected compromise of the Credentials;
- to notify without delay the Provider of any vulnerability, security breach or abnormal behavior of the Platform of which it becomes aware, and not to disclose it publicly before the Provider has been able to remedy it within a reasonable period.

9. CLIENT WARRANTIES

9.1 Warranties relating to Client Data and Prompts

The Client is solely responsible for the Client Data and Prompts it transmits to the Platform or makes accessible to the Agents. The Client warrants:

- to have all rights, licenses and authorizations necessary to process, transmit and allow the Platform to process such data and Prompts, without infringing the intellectual property rights, contractual or confidentiality obligations of any third party;
- that the Client Data and Prompts do not contain any unlawful, infringing, defamatory, pornographic content, content advocating violence, terrorism or any other offense, nor any content prohibited by the applicable regulations;
- that the transmission of such data and Prompts to the Platform and their processing by the latter do not contravene any sectoral regulation applicable to the Client, its sector of activity or the Underlying Clients;
- to comply with the terms of use of the websites for which it requests indexing in the RAG.

9.2 Guarantees relating to End Users and their data

The Client guarantees that any Conversation it transits through the Platform falls within a legal framework compliant with the applicable regulations, and in particular that it:

- has, or its Underlying Client has, a legal basis within the meaning of the GDPR to have the Platform process the personal data of End Users, including Audio, transcriptions, and any element resulting from the Conversations;

- a, or its Underlying Client has, fulfilled its information obligations towards End Users in accordance with Articles 12 to 14 of the GDPR, in particular regarding the identity of the controller, the purposes, the retention period, and the rights of the data subjects, as well as the rules applicable to the recording of telephone conversations in each relevant country;
- informs the Provider in advance, under the conditions of the DPA, of any Agent likely to process data falling under Articles 9 and 10 of the GDPR (notably health data), guarantees that the Underlying Client has a valid legal basis under Article 9.2 of the GDPR, configures a reduced retention period, favors the self-hosted LLM, and refrains from submitting such data to Copilot; the Provider may suspend any Agent not complying with these requirements;
- informs or has the End Users informed that they are interacting with an artificial intelligence system, in accordance with Article 50 of the AI Regulation.

9.3 Hold harmless guarantee and indemnification

The Client guarantees the Provider against any recourse, claim, action, conviction, or sanction that would result directly or indirectly from a breach of the guarantees given in Articles 4 bis.3, 5.2, 9.1 and 9.2 above, whether it originates from a third party, an End User, a supervisory authority, or any administrative or judicial authority.

In this respect, the Client undertakes to indemnify the Provider for all amounts that the latter may be required to incur as a result of such a breach, including defense costs, expert fees, amounts paid under a settlement approved by the Client, and judgments pronounced against the Provider.

10. FINANCIAL TERMS

10.1 Pricing

The Service is invoiced according to the current rates accessible on the Platform, or communicated by the Provider to the Client, applicable on the date of use of the Service. These rates notably cover the price per minute of Conversation, the Numbers, the pricing conditions applicable to the BYOK option, to the Storage at the Client option, and to optional features.

The Provider may modify the Service fees. Any fee modification is notified to the Client in writing, by any appropriate means, with a notice period of thirty (30) days before it takes effect. When the modification results in an increase in the fees applicable to the Client, the latter may terminate the Contract without penalty within thirty (30) days from the notification. If this option is not exercised within this period, the modified fees are deemed accepted and apply to the Client as of their effective date.

10.2 Invoicing and payment

Unless otherwise stipulated in the Order, invoices are issued monthly, at the end of each calendar month, based on the actual consumption of the Service during the elapsed month. Invoices are sent electronically to the address specified in the Order.

The default payment method is SEPA direct debit on the invoice issue date, unless otherwise stipulated in the Order.

10.3 Late payment

Any late payment automatically results, without prior formal notice and in accordance with the provisions of Article L. 441-10 of the Commercial Code, in the application of late payment penalties calculated on the basis of a rate equal to three (3) times the legal interest rate in force on the due date, as well as the payment of a fixed compensation for recovery costs of forty (40) euros per unpaid invoice. When the recovery costs incurred exceed this amount, the Provider may request additional compensation upon justification.

10.4 Invoice dispute

Any dispute relating to an invoice must be notified in writing to the Provider within thirty (30) days from receipt of the invoice, specifying the disputed items and the reasons for the dispute. Amounts not disputed within this period are deemed definitively accepted by the Client and remain payable at their due date. Partial dispute of an invoice does not suspend the obligation to pay undisputed amounts.

10.5 Electronic invoicing

The Parties undertake to comply with the electronic invoicing obligations applicable according to the legal schedule in force. In the event of a legal obligation to use a dematerialization platform, the Parties agree to adapt the invoice transmission procedures accordingly without the need for an amendment.

11. AVAILABILITY, SERVICE LEVELS AND MAINTENANCE

11.1 Service Level Commitments

The Service availability commitments, the terms of technical support, the severity levels of incidents, the response times, and any credits applicable in case of non-compliance are detailed in Appendix A. The Provider's commitments constitute obligations of means. They apply to all components of the Service provided by the Provider, whether the Provider operates them itself or entrusts their provision

to sub-processors that are inseparable from the Service identified in the DPA and in the Register of Sub-processors (notably hosting, speech recognition and speech synthesis), the Provider being answerable for those sub-processors as for itself under the service level commitments. They do not apply to the elements falling within the responsibility of the Client, its Underlying Clients or the third parties to whom they have recourse, under the conditions of Article 11.2.

11.2 Exclusions

Are expressly excluded from the calculation of availability and from any credit mechanism:

- the maintenance operations carried out by the Provider under the conditions of Article 11.3, whether planned or emergency;
- the unavailability resulting from an act of the Client, its Authorized Users, its Underlying Clients or their End Users, in particular in case of misuse, defective configuration, or failure of the Client's technical environment;
- the unavailability related to a malfunction of the public Internet network, to third-party telecommunications operators, to the telephone infrastructure connected by trunk SIP or to connectors, tools, and third parties connected at the Client's request, including as part of the BYOK option;
- the unavailability resulting from a case of force majeure within the meaning of Article 20;
- the unavailability of a feature in test phase, in beta, or not made available as part of a general availability phase.

By contrast, the unavailability resulting from a failure, a maintenance operation or any other event affecting a sub-processor that is inseparable from the Service mentioned in Article 11.1 is not excluded and is counted in the calculation of availability and in the credit mechanism, unless that event constitutes, in respect of that sub-processor, a case of force majeure within the meaning of Article 20.

11.3 Maintenance

The Provider regularly carries out preventive, corrective, or evolutionary maintenance operations on the Platform. Planned maintenance windows are, as far as possible, performed outside Working Hours and notified to the Client within reasonable timeframes. The Provider may, in case of technical or security necessity, carry out emergency maintenance operations without prior notice and will then inform the Client as soon as possible.

12. INFORMATION SYSTEM SECURITY

The Provider implements appropriate technical and organizational measures to ensure the security of the Platform and the data it processes, proportionate to the nature of the Service and the identified risks. These measures are described in the Provider's information system security policy, a summary of which is made available to the Client upon request, and, for personal data, in the corresponding appendix of the DPA.

Any audit request from the Client concerning the security of the Platform is handled as a priority by reference to the certifications, attestations, and independent audit reports held by the Provider. Audits relating to the processing of personal data are carried out under the conditions, timeframes, and billing terms set out in the DPA. Any other additional audit is subject to the prior agreement of the Parties on its scope and schedule and to remuneration at the Client's expense.

13. PERSONAL DATA

The performance of the Service leads the Provider to process personal data within the meaning of Regulation (EU) 2016/679 ('GDPR') on behalf of the Client, as a processor or sub-processor depending on whether the Client acts for its own needs or for those of its Underlying Clients. These processing operations are exclusively governed by the DPA, which specifies the qualification of the Parties, instructions, security measures, sub-processors, transfers, assistance, notification of personal data breaches, audits, and the fate of the data. The register of sub-processors and the location of their processing are kept up to date in the Register of Sub-processors, accessible in the Legal area of the Console and, for consultation in the form of a neutral list, from the Client Portal; the Client relays its content to Underlying Clients who do not use the Client Portal, under the conditions of the DPA.

Data relating to the Client's account, its Authorized Users, billing, and the commercial relationship are processed by the Provider as controller, in accordance with its privacy policy accessible on the Platform. The Provider's specific obligations as an electronic communications operator (Article 4 bis) are performed independently of the DPA.

The liability caps provided for in Article 17 are not affected by the provisions of the DPA, subject to the specific guarantees that the latter imposes on the Client.

14. PROVISIONS RELATING TO AGENTS AND THE AI REGULATION

14.1 Probabilistic Nature of Outputs

The Outputs generated by the Agents result from the combination of the Client's Prompts, the Provider's proprietary components, and the capabilities of the LLM applied to the Conversations. These Outputs result from probabilistic reasoning likely to contain approximations, inaccuracies, omissions, or erroneous information (phenomena sometimes referred to as « hallucinations »).

The same applies to transcriptions resulting from speech recognition, which may contain transcription errors, and to automatic summaries, which may omit or imperfectly rephrase elements of the Conversations. The Client is expressly informed of these limitations and accepts the consequences thereof.

14.2 Roles of the Parties with regard to the AI Regulation

The roles defined by the AI Regulation are independent of those defined by the GDPR and depend in particular on the name or brand under which the artificial intelligence system is placed on the market. Without prejudice to the qualification resulting from the facts, the Parties agree as follows:

- Option 1 (marketing under the Brand): the Provider is the supplier of the Platform and the Agents placed on the market under the Brand; the Client and its Underlying Clients are deployers of the Agents that they configure and operate under their authority;
- Option 2 (White Label): the Client, who places the artificial intelligence system on the market under its own name or brand, is a supplier within the meaning of Article 3(3) of the AI Regulation; the Provider is an upstream supplier of the Platform and its components and provides the Client, pursuant to Article 25(4) of the AI Regulation and under the conditions of the DPA, with information relating to the capabilities, limitations, and conditions of use of the Platform necessary for the performance of its obligations, subject to its trade secrets.

14.3 Transparency and marking of generated content

The Platform allows End Users to be informed that they are interacting with an artificial intelligence system, in particular by means of the configurable welcome message of each Agent; the Client is responsible for the effective activation and wording of this information in each Agent, in accordance with Article 50 of the AI Regulation. The Provider implements, to the extent technically possible given the constraints of telephony and the state of the art, the machine-readable marking measures for generated audio content provided for in Article 50(2) of the AI Regulation, the limitations of which it documents; the Client shall refrain from disabling or altering them.

14.4 Classification of Agents

The classification of Agents with regard to the AI Regulation depends on the use case pursued by the Client or, where applicable, by its Underlying Client. Uses falling under Annex III of the AI Regulation are prohibited without the prior agreement of the Provider under the conditions of Article 7.2. Where a use case entails additional obligations for the Provider, the Provider may make contractual adjustments a condition thereof or, failing agreement, suspend the Agent concerned under the conditions provided for in Article 18.

15. INTELLECTUAL PROPERTY

15.1 Provider's proprietary assets

The Provider is and remains the sole holder of all intellectual property rights relating to the Platform, and in particular:

- the source code and object code of the Platform;
- the RAG and the associated algorithmic components;
- the parameters, rules and technical instructions specific to the orchestration of the audio pipeline;
- the Console, the Client Portal and their ergonomics;
- the documentation, the Brand, other trademarks, logos, trade names and any other distinctive sign of the Provider;
- any evolution, improvement, correction or adaptation of the aforementioned elements.

The Contract does not grant the Client any ownership rights over these elements, but only the right of use defined in Article 15.2 and, where applicable, the Brand license defined in Article 15 bis.

15.2 License of use granted to the Client

Subject to the Client's compliance with its contractual obligations and in particular the payment of amounts due, the Provider grants the Client, for the duration of the Contract, a right of access and use of the Platform on a non-exclusive, personal, non-transferable and non-sublicensable basis, it being specified that the Client may grant access to its Authorized Users and its Underlying Clients under the conditions set out in Article 8.

This right is granted worldwide and strictly for the execution of the use cases provided for in the Contract. It ends automatically upon termination of the Contract, regardless of the cause.

15.3 Client's proprietary assets

The Client retains exclusive ownership of the Client Data and Prompts that it makes available to the Platform. The Provider acquires no rights over these elements as a result of their processing by the Platform.

The Client grants the Provider, solely for the purposes of performing the Service, a right to use, reproduce, transmit, host and technically adapt the Client Data and Prompts strictly to the extent necessary to provide the Service to the Client. This license ends with the termination of the Contract, subject to the Provider's legal retention obligations.

15.4 Restrictions

The Client is prohibited from:

- from reproducing, adapting or modifying the Platform and the Provider's proprietary assets referred to in Article 15.1, except within the limits of the rights granted by law;
- from carrying out or having carried out reverse engineering, disassembly or decompilation operations on the Platform, except under the strictly defined conditions of Article L. 122-6-1 of the Intellectual Property Code;
- to use the Platform or the Outputs to train, fine-tune or enrich a competing artificial intelligence model;
- to sub-license, rent, lend or resell access to the Platform to third parties outside the conditions set forth in Article 8.

15 bis. BRAND AND COMMERCIALISATION REGIME

The Client markets the Service to its Downstream Clients according to one of the following two regimes, chosen in the Order. The Brand Regime has no impact on the roles of the Parties under the GDPR, governed by the DPA, but determines their roles under the AI Regulation (Article 14.2).

15 bis.1 Option 1 — Commercialisation under the Brand

The Provider grants the Client, for the duration of the Contract and solely for the purposes of marketing the Service to its Downstream Clients, a non-exclusive, non-transferable and non-sublicensable license to use the Brand, as registered and in compliance with the graphic charter communicated by the Provider. The Client is prohibited from modifying the Brand, associating it with signs that damage its image, registering any identical or similar trademark, denomination or domain name, and from using it beyond the term of the Contract. The Client informs its Downstream Clients that the Service is provided by the Provider under the Brand and that the Client remains their sole contracting party, subject to the assignment of the Numbers (Article 4 bis.1), under the conditions set forth in the DPA.

15 bis.2 Option 2 — White Label

The Client markets the Service under its own brand, without reference to the Provider or the Brand to the End Users. The Client Portal made available by the Provider is an optional feature, the use of which is in no way a condition for the Client's marketing of the Service to its Downstream Clients. When the Client uses the Client Portal, the customization offered by the Platform is limited to the replacement of the logo Manivox by that of the Client in the Console and the Client Portal; the Client Portal remains hosted on the manivox.ai domain and the name Manivox may appear there (address, technical mentions), which the Client accepts and brings to the attention of its Downstream Clients. The Client who wishes to offer its Downstream Clients an interface entirely under its own brand and its own domain name may, instead of the Client Portal, develop its own interface hosted on its infrastructure

and consuming the Platform APIs, under the conditions set forth in Article 4.1; the Provider does not intervene in the hosting or the domain name of this interface. The Client remains obliged to inform its Downstream Clients of the identity of the Provider as sub-processor; Downstream Clients using the Client Portal consult the Register of Processors (neutral list) directly, and the Client relays its content to those who do not have access, under the conditions of the DPA. The Client guarantees that it holds the rights to the brand and logo it uses and indemnifies the Provider against any claim in this respect.

15 bis.3 Change of Regime

The Client may change the Brand Regime by giving the Provider sixty (60) days' prior written notice, subject to the applicable pricing conditions and the update of the Order. The transition from Option 1 to Option 2 entails the termination of the Brand license at the expiration of the notice period.

16. CONFIDENTIALITY

Confidential information includes any information communicated by one Party to the other under the Contract and expressly designated as such.

The following are also considered confidential, without the need for express designation: for the Provider, the RAG, technical parameters, source code, Platform architecture, processing and orchestration methods, pricing conditions, technical know-how, and any document marked as confidential; and for the Client, the Client Data, Prompts, knowledge bases, business strategy, information relating to Underlying Clients and End Users, as well as Conversations and their Outputs.

Each Party undertakes to maintain the other Party's confidential information in strict confidence, not to disclose it to third parties without prior written consent, and to use it solely for the purposes of performing the Contract. This obligation applies throughout the duration of the Contract and for five (5) years after its termination.

Each Party undertakes to authorize access to confidential information only to persons who have a legitimate need to know for the performance of the Contract, and to ensure that such persons are subject to confidentiality obligations at least equivalent to those provided for in this article.

The confidentiality obligations do not apply to information that is or becomes public without fault of the receiving Party, that was already legitimately known to the receiving Party before disclosure, that is lawfully received from a third party without confidentiality obligation, or that must be disclosed pursuant to a legal or regulatory obligation or a decision of a competent authority. In the latter case, the Party required to disclose shall inform the other Party as soon as possible and limit the disclosure to what is strictly necessary.

17. LIABILITY AND WARRANTIES

The Provider's total cumulative liability to the Client under the Contract, for all causes combined, is limited to the total amount actually paid by the Client to the Provider under the Contract during the one (1) month preceding the event giving rise to the damage. This limitation reflects the allocation of risks between the Parties, which has been taken into account in determining the price of the Service.

The Provider cannot be held liable for indirect damages suffered by the Client or by third parties, including but not limited to loss of business, revenue, margin, profits, anticipated savings, clientele, markets or contracts, loss or alteration of data, damage to image or reputation, consequences of any action brought by a third party against the Client, nor for fines, sanctions or administrative, regulatory or criminal penalties imposed on the Client.

The Provider is not liable for damages resulting from the probabilistic nature of the Outputs, from non-compliant use of the Platform, from inaccurate, incomplete, unlawful Client Data or Prompts or provided in violation of third-party rights, from a lack of information to the End User attributable to the Client or its Underlying Client, from a failure of an LLM or a third-party tool brought by the Client under the BYOK option, from a failure of the Client's storage infrastructure under the Client Storage Option, from a non-compliant Outbound Campaign, from a failure of the Client's technical environment or third-party tools connected to the Platform at its request, nor from a case of force majeure within the meaning of Article 20.

The limitations and exclusions of liability provided for in this article also apply to the Provider's breaches of the DPA, under the conditions set forth therein; the specific warranties granted by the Client under the DPA and Articles 4 bis.3, 5.2 and 9 are not subject to the above cap. The limitations and exclusions of liability do not apply in cases of willful misconduct, gross negligence or harm to persons, to the extent that the law prohibits the exclusion or limitation of liability in such cases.

18. TERM, SUSPENSION AND TERMINATION

18.1 Term

The Contract enters into force on the date specified in the Order, for the initial term agreed therein. At the end of the initial term, the Contract is renewed by tacit agreement for successive periods corresponding to the duration specified in the Order, unless terminated by either Party under the conditions of this article.

18.2 Termination at the Client's initiative

The Client may terminate the Contract at the end of the initial term, on each anniversary date, subject to notice given in writing to the Provider at least three (3) months before the due date. All amounts due for the period prior to the effective date of termination and for the notice period remain payable,

and no refund of prepaid amounts shall be due.

By way of exception, the Client may terminate the Contract without penalty, by written notice and with effect on the date indicated by the Client, in the cases provided for by the DPA: a justified objection based on data protection to the addition or replacement of a sub-processor that is inseparable from the Service, or refusal of a substantial modification of the DPA reducing the level of data protection. In these cases, amounts corresponding to the period after the effective date of termination are not due and the corresponding prepaid amounts are refunded on a pro rata basis.

18.3 Termination for breach

Each Party may terminate the Contract as of right, by registered letter with acknowledgment of receipt, in the event of a serious breach by the other Party of any of its obligations that has not been remedied within fifteen (15) days from receipt of a formal notice that has remained without effect, without prejudice to any damages.

The Provider may terminate the Contract without prior formal notice in the event of unlawful, fraudulent, or public order-contrary use of the Platform, as well as in the event of non-payment of an undisputed invoice that remains unpaid for more than five (5) days after formal notice.

18.4 Suspension

The Provider may suspend access to the Platform, to an Agent, or to an Outbound Campaign, without prejudice to its right to termination, in the event of non-payment of an undisputed invoice remaining unpaid for more than fifteen (15) days after its due date, in the event of a material breach of the acceptable use conditions provided for in Article 7 or in Articles 4 bis.3, 9.2 and 14.4, in the event of a security emergency, or upon instruction from a competent authority. Suspension does not prevent the amounts due under the Contract from becoming payable. When the cause of the suspension is not remedied within thirty (30) days, the Provider may terminate the Contract as of right.

18.5 Effects of termination

Termination, whatever the cause, entails the immediate payment of all amounts due, the cessation of the right of access to the Platform and of the Brand license, the disconnection of Authorized Users and Clients Underlying, the return of the Numbers or, at the request of their assignee, their porting, under regulatory conditions and those of the mandate provided for in Article 4 bis.1, as well as the implementation of the reversibility operations and deletion of the Client's Data provided for below.

18.6 Fate of the Client's Data

From the termination of the Contract, the Provider shall, at the Client's choice expressed under the conditions of the DPA, either return in a structured and commonly used format or securely delete the Client's Data present in its systems, including backups, within thirty (30) days, and shall provide, upon request, a certificate of deletion. The Provider ceases to write to the Storage infrastructure at the Client, the content of which remains under the sole control of the Client. The Provider may retain the Client's Data relating to the performance, invoicing, and payment of the Service, as well as the traffic data it retains as an operator, for the minimum period required by its legal obligations.

19. AMENDMENT OF THE GENERAL TERMS AND CONDITIONS

The Provider may amend these General Terms and Conditions to take into account changes in the Service, applicable regulations, or market practices.

The amendments are notified to the Client by any written means, with reasonable prior notice, which may not be less than sixty (60) days when the amendments substantially affect the rights or obligations of the Client.

Amendments made necessary by a legal or regulatory obligation may be implemented without prior notice, with the Client being informed by any appropriate means.

When the amendments substantially and adversely affect the rights of the Client, the latter may, within thirty (30) days from the notification, notify the Provider in writing of its refusal to accept them, such refusal resulting automatically in the termination of the Contract on the effective date of the amendments, without penalty.

Changes to the functional scope and price revisions remain governed, respectively, by Articles 4.2 and 10.1. Amendments to the DPA are governed by the DPA itself, with the same sixty (60) day notice period.

20. FORCE MAJEURE

Neither Party shall be held liable for a failure to fulfill its obligations resulting from a case of force majeure within the meaning of Article 1218 of the Civil Code, as interpreted by the case law of the French courts.

The following are notably considered as cases of force majeure, without this list being exhaustive: armed conflicts, acts of terrorism, riots, pandemics, epidemics, natural disasters, decisions of public authorities affecting the performance of the Contract, widespread failures of the Internet network or public telephone networks, failures of the hosting infrastructure or of a third-party provider in the technical chain of the Service, provided that they themselves result from an event presenting, in respect of that provider, the characteristics of force majeure, cyberattacks making it temporarily impossible to perform the Service, material shortages affecting the technical components underlying

the Service.

The Party invoking a case of force majeure shall inform the other Party as soon as possible and specify the expected consequences on the performance of the Contract. The Parties shall seek in good faith solutions to continue the performance of the Contract. If the force majeure event continues for more than thirty (30) days, each Party may terminate the Contract automatically, without penalty, by written notification to the other Party.

21. MISCELLANEOUS PROVISIONS

Assignment. The Client may not assign the Contract, in whole or in part, nor transfer its rights and obligations to a third party, without the prior written consent of the Provider. The Provider may assign the Contract to any company within its group or to a third-party acquirer, in the event of a merger, demerger, partial transfer of assets or transfer of business, subject to informing the Client and provided that the assignee assumes all of the Provider's obligations under the Contract.

Sub-processing. The Provider may use technical processors for the provision of the Service, in particular for hosting components, speech recognition, speech synthesis, connectors, and optional artificial intelligence assistance functions. These processors are identified in the DPA and in the Register of Processors, and not herein, so that their replacement is carried out according to the procedure in the DPA without modification of the General Terms and Conditions. The Provider remains responsible for the provision of the Service to the Client.

Independence of the Parties. The Parties are independent contractors. The Contract does not create between them any company, mandate, joint venture, agency or representation relationship, nor any employment relationship.

Entire Agreement. The Contract constitutes the entire agreement between the Parties relating to its subject matter and supersedes any prior agreement, exchange or representation, written or oral, relating to the same subject matter.

No Waiver. The fact that one Party does not invoke a breach by the other Party of any of its obligations shall not be interpreted as a waiver of the right to invoke such breach or any subsequent breaches. Any waiver must, in order to be effective, be express and in writing.

Severability. If any provision of the Contract is declared null, illegal or unenforceable by a court decision or as a result of a legislative or regulatory change, the other provisions shall remain in full force and effect.

Notifications. Any notification under the Contract is validly made by registered letter with acknowledgment of receipt or by email with acknowledgment of receipt or delivery notice, to the addresses specified in the Order, as well as, for notifications from the Provider relating to sub-processors and Service changes, by notification in the Console together with an email. Any change of

address must be notified to the other Party in the same manner.

Electronic signature. The Parties agree that the Order and any other contractual document may be signed electronically. An electronic signature affixed in accordance with the applicable European and French regulations has the same legal value as a handwritten signature and is accepted as evidence between the Parties. The use of an advanced or qualified electronic signature process is deemed sufficient. Each signatory confirms that they have the authority to represent and bind the Party in whose name and on whose behalf they are signing.

Evidence agreement. The Parties agree that computer records, event logs, and files kept by the Provider in the context of operating the Platform, including the timestamped certificates provided for in Article 4 bis.3, are binding between them and constitute admissible evidence within the meaning of Article 1366 of the Civil Code, unless proven otherwise.

Language. The Contract is drafted in French, which constitutes the authoritative version between the Parties. In the event of a translation of the Contract into another language for convenience, the French version shall prevail in case of any discrepancy in interpretation.

Governing law. The Contract is governed by French law, to the exclusion of any conflict of law rules that would lead to the application of another law.

Dispute resolution and competent courts. In the event of a dispute relating to the interpretation, performance, or termination of the Contract, the Parties undertake to approach each other in good faith with a view to finding an amicable solution. Failing an amicable agreement within thirty (30) days from the written notification of the dispute by one Party to the other, any dispute shall be submitted to the exclusive jurisdiction of the courts within the jurisdiction of the Paris Court of Appeal, notwithstanding multiple defendants or third-party proceedings.

ANNEX A — SERVICE LEVELS (SLA)

This annex sets out the Provider's service level commitments, the terms of technical support, and the credits applicable in the event of non-compliance.

1. Availability

The Provider undertakes to ensure Platform availability of 99.5% calculated per calendar month according to the following formula: $\text{Availability (\%)} = \frac{[(\text{Total time of the calendar month} - \text{Downtime}) / \text{Total time of the calendar month}] \times 100}{100}$.

Total time and Downtime are expressed in minutes. A period of unavailability means any continuous interruption lasting more than five (5) minutes, excluding the periods mentioned in Article 11.2 of the General Terms and Conditions, during which (i) all or part of the Agents put into service by the Client

cannot receive or place calls or process Conversations, notably due to a failure of telephony, speech recognition, the self-hosted LLM or speech synthesis, or (ii) the Console is inaccessible. Periods of unavailability are established by means of the Provider's monitoring tools, the records of which are communicated to the Client upon request, or by any supporting evidence produced by the Client.

2. Support

The Provider ensures technical support accessible via the Console and, where applicable, by other means specified in the Order or on the Platform. The Provider undertakes, from the receipt of the report and during Business Hours, to comply with the following response times depending on the severity of the malfunction:

Level	Definition	Response time
P1 — Blocking	Total unavailability of the Service or impossibility to use an essential feature, with no possible workaround.	1 hour
P2 — Major	Significant degradation of an essential feature, with a possible but uncomfortable workaround.	4 hours
P3 — Minor	Malfunction not substantially affecting the use of the Platform (cosmetic anomaly, request for information, occasional inconvenience).	8 business hours

Any report received outside Business Hours is deemed received at the first following business hour. The Provider may reclassify the severity of a malfunction reported by the Client in light of the above criteria. The above deadlines correspond to the response to the report and not to the resolution time of the malfunction, which depends on its nature and cause.

3. Credits in case of non-compliance

In the event of non-compliance with the availability rate provided for in Article 1 of this annex for a given calendar month, the Client may claim, upon written request made within thirty (30) days following the end of the relevant calendar month and accompanied by the necessary supporting documents, a credit equal to five percent (5%) of the amount invoiced for the relevant calendar month. This credit is applied to the invoice for the following calendar month.

The cumulative amount of credits owed by the Provider under this annex may not, in any event, exceed ten percent (10%) of the total amount invoiced annually to the Client for the relevant calendar year.

The credit provided for in this article constitutes the sole and exclusive remedy due by the Provider in the event of non-compliance with the service level commitments, to the exclusion of any damages,

indemnity or other form of compensation, except in cases of gross negligence or willful misconduct by the Provider or termination for serious breach under the conditions provided for in Article 18.3 of the General Terms and Conditions.

4. Option Storage at the Client, BYOK option and trunk SIP

When the Client has implemented the Option Storage at the Client (Article 6.1 of the General Terms and Conditions), the commitments of this annex do not cover the portion of storage relating to the Client's infrastructure. When the Client has recourse to the BYOK option (Article 5.2 of the General Terms and Conditions), unavailability of the LLM or third-party tools provided by the Client are not counted in the calculation of the availability of the Platform and do not give rise to any credit. The same applies to unavailability attributable to the telephone infrastructure connected by trunk SIP (Article 4 bis.2). By contrast, unavailability attributable to the Provider's sub-processors that are inseparable from the Service is counted under the conditions of Articles 11.1 and 11.2 of the General Terms and Conditions.

ANNEX B — CORRESPONDENCE TABLE T&Cs ↔ DPA

These General Terms describe the commercial relationship; the DPA describes the processing of personal data. The following correspondences apply between their defined terms. In case of doubt regarding a data protection matter, the definition in the DPA prevails; for any other matter, that of the General Terms.

Term of the T&Cs	Term of the DPA	Accuracy
Provider	Manifone / Processor	Same legal entity, operating under the brand Manivox.
Client	Distributor	The DPA designates it as Distributor whether it acts for its Underlying Clients or for its own needs.
Underlying Client	End Client	Controller in the general case; covers any client on whose behalf an Agent is operated, whether or not it accesses the Platform.
End User	Data Subject	The DPA concerns any natural person whose personal data are processed, beyond the sole contacts of the Agents.
Authorised User of an Underlying Client	User of the Client Portal	Accounts created under Article 8.
Contract (Order + TOS + DPA + appendices)	Framework Agreement	—

Term of the T&Cs	Term of the DPA	Accuracy
Order	Order / Appendix 6 of the DPA	The information in Annex 6 of the DPA is included in the Order or entered in the Console.
Platform / Service	Platform Manivox / Service	—
Console (view Underlying Clients)	Console / Client Portal	—
Client Data, Conversations, Audio, Outputs	Data	The DPA only retains the personal data component.
Audio / transcriptions / summaries	Audio recordings / transcriptions / call summaries	—
Prompts	Conversational flow, script	—
Connector integrated into the Platform	Connector	Integration platform identified in the DPA (Annex 2a) and in the Register of Processors.
BYOK Option / API Key	Provider or third party connected in BYOK mode	Extended to any third party connected by the Client (Article 5.2; Article 9.4 of the DPA).
Storage Option at the Client	Storage at the Client	—
Brand Regime (Option 1 / Option 2)	Brand Regime (Option 1 / Option 2)	Articles 15 bis of the GTCU and 4 of the DPA.
AI Regulation	AI Act	Same text: Regulation (EU) 2024/1689.
Register of Processors (Legal area of the Console)	Register of Processors	—

ANNEX C — CONTRACTUAL BASELINE APPLICABLE TO UNDERLYING CLIENTS

This appendix lists the provisions that the Client includes, in substance, in the contract binding it to each of its Underlying Clients, in accordance with Article 8.2, whether or not the Underlying Client accesses the Platform. The Client remains free as to the drafting, structure and form of that contract, as well as as to any provision not contrary to this baseline. The Provider may make available to the Client an optional model contract, provided for guidance only and without any warranty as to its suitability to the Client's particular situation, which the Client adapts under its sole responsibility. The Provider is not a party to the contract entered into between the Client and the Underlying Client; only the assignment of the Numbers to the Underlying Client, ordered by the Client as agent of the latter (Article 4 bis.1), creates a direct relationship between the Provider and the Underlying Client.

C.1 — Professional capacity

The Underlying Client declares that it acts exclusively in a professional capacity, for the purposes of its business.

C.2 — Acceptable use

The Underlying Client undertakes to comply with prohibitions equivalent to those of Article 7.2, and in particular: not to have configured or operated any Agent falling within the high-risk artificial intelligence systems referred to in Annex III of the AI Regulation without the prior written agreement of the Client, itself subject to the agreement of the provider of the technical platform; not to resort to the practices prohibited by Article 5 of the AI Regulation; not to have unlawful content disseminated; and to ensure the lawfulness of the Outbound Campaigns configured on its behalf, in particular with regard to the prior consent regime of Article L223-1 of the Consumer Code and the rules relating to days, times and frequencies of canvassing.

C.3 — Information of End Users and deployer obligations

The Underlying Client, controller in the general case, ensures the information of End Users under Articles 13 and 14 of the GDPR, including as regards the recording of telephone conversations. It ensures that End Users are informed, from the beginning of the conversation, that they are interacting with an artificial intelligence system, unless this is obvious from the context (Article 50 of the AI Regulation), and to that end determines or validates the greeting message of each of the Agents operated on its behalf. In its capacity as deployer within the meaning of the AI Regulation, it also ensures that the members of its staff concerned have a sufficient level of AI literacy (Article 4 of the AI Regulation).

C.4 — Data processing agreement

The Client and the Underlying Client enter into a processing agreement compliant with Article 28.3 of the GDPR, containing data protection obligations substantially equivalent to those of the DPA (Article 3.1 of the DPA), and in particular:

- the general written authorization, given by the Underlying Client, for the Client to use the Provider as a sub-processor and for the latter to use its own sub-processors, the list of which appears in the Register of Sub-processors;
- the passing on without delay to the Underlying Client of any notification of the addition or replacement of a sub-processor received from the Provider pursuant to Article 9 of the DPA, under conditions enabling the Underlying Client to exercise its right of objection effectively;
- assistance, notification of data breaches, audit and the fate of the data at the end of the contract, under conditions compatible with those of the DPA.

C.5 — Confidentiality of the identity of sub-processors

The Underlying Client treats as confidential the information relating to the identity of the sub-processors and the location of their processing operations that is communicated to it, uses it only to satisfy its own obligations under the applicable regulations, and discloses it only to its advisers, to the competent authorities and, where applicable, to data subjects to the extent strictly required by those regulations.

C.6 — Sensitive data

The Underlying Client informs the Client, prior to the entry into service of any Agent, that that Agent is likely to process data falling within Articles 9 or 10 of the GDPR, and warrants that it has a valid legal basis under Article 9.2 of the GDPR as well as the required authorizations or formalities.

C.7 — Connection credentials for third-party tools

Where the Client itself enters the Underlying Client's connection credentials for the third-party tools connected to the Agents, the Underlying Client expressly authorizes it to do so, warrants that it has the right to communicate them having regard to the terms of use of those tools, and remains responsible for the authorizations thus granted and for their revocation. The contract mentions, where applicable, the ability for an Underlying Client having access to the Client Portal to enter those credentials directly (Article 8.3).

C.8 — Intellectual property and integrity of the service

The Underlying Client has no right over the Platform, its components and the Brand, other than the right to use the service granted to it by the Client. It is prohibited from any reverse engineering, decompilation, extraction or attempted unauthorized access, as well as from any use of the service with a view to developing a competing product or service.

C.9 — Suspension and cessation of the service

The Underlying Client is informed that the service relies on a technical platform supplied by a third party, that the Agents operated on its behalf may be suspended in the cases provided for in the contract binding the Client to that supplier (in particular non-compliant use, security emergency, instruction from a competent authority or non-payment by the Client), and that the termination of that contract entails that of the service. The contract organizes the reversibility of the Underlying Client's data under conditions compatible with Article 20 of the DPA.

C.10 — Role of the platform supplier according to the Brand Regime

- Option 1 (Brand): the contract informs the Underlying Client that the service is provided by means of the Manivox platform, published by the Provider, which acts in the capacity of technical sub-processor within the meaning of the GDPR and of provider of the artificial intelligence system within the meaning of Article 3(3) of the AI Regulation, and that the Client remains its sole contracting party, subject to the assignment of the Numbers (point C.11); the visibility of the Brand entails no

other direct relationship between the Underlying Client and the Provider.

- Option 2 (White Label): the contract identifies the Provider in the capacity of sub-processor within the meaning of the GDPR, without any obligation to mention it to End Users, a designation by category being sufficient as regards them; an Underlying Client that accesses the Client Portal is informed that the latter is hosted on the manivox.ai domain and that the name Manivox may appear there.

C.11 — Numbers

The Underlying Client signs electronically, prior to any order of Numbers on its behalf, the Numbers management mandate provided for in Article 4 bis.1. The contract informs it, whatever the Brand Regime, that it becomes the assignee of the Numbers ordered on its behalf, that the Provider is the operator of those Numbers, and that the termination of the contract entails the termination of those Numbers, unless it exercises its right to retain its numbers.

The provisions of this appendix are without prejudice to the rights that data subjects derive directly from the regulations, in particular from Article 82 of the GDPR.

ANNEX D — ESSENTIAL PROVISIONS OF THE NUMBERS MANAGEMENT MANDATE

The template Numbers management mandate made available in the Console may evolve, in particular to take account of regulatory developments. Any version of that template contains at least the following provisions, which the Client may neither delete nor modify. The mandate is entered into between the Underlying Client, as principal, and the Client, as agent; the Provider is not a party to it, the provisions of points D.7 and D.8 being stipulated for its benefit.

D.1 — Purpose and powers

The principal gives the agent the power to order from the Provider Numbers of which the principal becomes the assignee within the meaning of the national numbering plan, to terminate them, to modify their settings and to present them on calls made on its behalf.

D.2 — Regulatory basis

The mandate recalls the rules that require the assignment of the Numbers to the professional on whose behalf they are used, in particular Article L221-17 of the Consumer Code for outgoing calls and the rules for managing the national numbering plan laid down by the Regulatory Authority for Electronic Communications, Postal Services and Print Media Distribution, and specifies that it applies to all categories of Numbers.

D.3 — Contractual context

The mandate recalls the existence of the Contract between the Provider and the agent, and of the service contract between the agent and the principal. The financial conditions fall exclusively within those two contracts; the principal owes no sum to the Provider under the mandate.

D.4 — Notifications

The mandate designates an email address of the principal and an email address of the agent, to which the Provider notifies orders, assignments, terminations and portings of Numbers as well as changes to the data depending on the principal, in particular the address to which the Numbers are attached, excluding changes to technical settings.

D.5 — Rights of the assignee

Only the principal, in its capacity as assignee, is entitled to retain its Numbers in the event of a change of operator or of agent. It may request the Provider directly to terminate or port its Numbers.

D.6 — Duration and cessation

The mandate terminates automatically in the event of cessation of the contract between the principal and the agent or of the Contract between the Provider and the agent. Its cessation, whatever the cause, entails the termination of the Numbers with the Provider, unless a porting request is made by the principal; the agent carries out that termination without delay from the Console.

D.7 — Outgoing calls

The principal and the agent undertake to comply with the regulations on telephone canvassing and automated calls, in particular Articles L221-16, L221-17 and L223-1 et seq. of the Consumer Code, as well as the rules of the Regulatory Authority for Electronic Communications, Postal Services and Print Media Distribution relating to the use of Numbers for such calls.

D.8 — Provisions for the benefit of the Provider

The Provider may terminate the Numbers covered by the mandate in the event of non-payment by the agent, after a formal notice has remained unsuccessful, as well as in the event of repeated and reported breaches of the regulations referred to in point D.7; a breach by the principal of those regulations gives rise to a right to compensation for the loss resulting therefrom for the Provider.

D.9 — Personal data

The mandate informs the principal, under Article 14 of the GDPR, of the processing carried out by the Provider in the capacity of controller on the identification data of the principal, of its signatories and of the recipients of the notifications, as well as on the traffic data relating to the Numbers, for the management of numbering resources and the performance of its legal obligations as an operator, and refers to the Provider's privacy policy.

D.10 — Signature, retention and applicable law

The mandate is signed electronically by the principal and the agent by means of the electronic signature process implemented by the Provider in the Console, which ensures the authentication of the signatory, in particular by a one-time code sent to its email address, and the integrity of the signed mandate. The mandate contains an evidence agreement under which the principal and the agent acknowledge the evidential value of that process and of the evidence file retained by the Provider, comprising in particular the identity and email address of the signatory, the timestamp of the sending and of the entry of the one-time code, the timestamp of the signature and the hash of the signed document. The Provider retains the signed mandate and its evidence file for the duration of the assignment of the Numbers and the applicable limitation period; it keeps them available to the agent and communicates them to the principal on request. The mandate is governed by French law.