Once fully executed, this Data Processing Agreement forms a part of the Agreement between the PROVIDER and the CLIENT for the provision of PROVIDER's Services.

HOW TO EXECUTE THIS DATA PROCESSING AGREEMENT:
This Data Processing Agreement has been pre-signed on behalf of the PROVIDER.

To complete this Data Processing Agreement, the CLIENT needs to:

1. Complete the information as the " CLIENT " on page 1
2. Complete the signature box and sign on page 6
3. Send the completed and signed Data Processing Agreement to the PROVIDER at the email address Administration_Signatures@infobip.com.

Upon receipt of the validly completed and signed Data Processing Agreement at the email address indicated above, it will become legally binding. If you decide to use **electronic signature**, make sure to use a valid one (e.g., a copied-and-pasted image of a signature on a PDF is not a valid form).

In case of additional information or inquiries please contact: gdpr_legal@infobip.com.

DATA PROCESSING AGREEMENT

This **"Data Processing Agreement"** (hereinafter: DPA) is made and entered into between **INFOBIP LTD** (CRN: 7085757), a company registered in the United Kingdom and whose registered office is situated at 5th Floor, 35-38 New Bridge Street London EC4V 6BW, hereinafter referred to as "Infobip" or "PROVIDER".

And

_____{**COMPANY NAME, REGISTRATION NUMBER**} a company registered in _____{COUNTRY} and whose registered office is situated in _____{PHYSICAL ADDRESS} and duly represented by_____{COMPANY REPRESENTATIVE'S FIRST AND LAST NAME, and JOB TITLE}, hereinafter referred to as " CLIENT " and together with PROVIDER, the "Parties".

INTRODUCTION

Whereas

a) The Parties have entered into one or more agreements for the provision of the Services / Terms & Conditions by PROVIDER to the CLIENT (hereinafter: **"Agreement"**),

b) In the course of providing PROVIDER Services as defined in the Agreement, it is necessary for PROVIDER to process certain personal data on behalf of the CLIENT, who may act as a controller or as a processor of personal data as defined under the Applicable Data Protection Law (specified hereunder),

the Parties have entered into this Data Processing Agreement (hereinafter: **"DPA"**) and agreed as follows:

1. DEFINITIONS

a) "**Applicable Data Protection Law**" shall mean all laws and regulations applicable to the processing of personal data under this DPA, including, where applicable, the GDPR (General Data Protection Regulation (EU) 2016/679), the UK GDPR, the UK Data Protection Act 2018, and any laws and regulations implementing the foregoing, as amended or superseded from time to time.

b) "**US Privacy Law**" shall mean all laws and regulations of the United States applicable to the processing of personal data, including, where applicable, the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA"); the Virginia Consumer Data Protection Act ("VCDPA"); the Colorado Privacy Act ("CPA"); the Utah Consumer Privacy Act ("UCPA"); the Connecticut Act Concerning Personal Data Privacy and Online Monitoring ("CTDPA"); the Telephone Consumer Protection Act ("TCPA"); the Controlling the Assault of Non-Solicited Pornography And Marketing Act ("CAN-SPAM"); the Electronic Communications Privacy Act; Massachusetts Gen. Law Ch. 93H, and any laws and regulations implementing the foregoing, as amended or superseded from time to time.

c) "**Personal Data**" shall mean any information relating to an identified or identifiable natural person (hereinafter: "**Data Subject**") and other personal information as defined by Applicable Data Protection Law when processed on behalf of the CLIENT.

d) "**PROVIDER Services**" shall have the meaning ascribed to it in the Agreement, to the extent where the provision of PROVIDER Services implies the processing of Personal Data on behalf of the CLIENT as described in Annex 1.

e) The terms used in this DPA, such as (but not limited to) "**processing**", "**controller**", "**processor**", "**third party**", "**personal data breach**" and "**technical and organizational measures**", shall have the meaning ascribed to them in the Applicable Data Protection Law.

2. DETAILS OF THE PERSONAL DATA PROCESSING

2.1. If and to the extent that PROVIDER will be processing Personal Data on behalf of the CLIENT in the course of the performance of PROVIDER Services, an overview of the nature, purposes, and duration of the processing, types of Personal Data, categories of Data Subjects, and other details regarding the processing are provided in Annex 1, insofar as they are not already described in the Agreement.

3. OBLIGATIONS OF THE CLIENT

3.1. The CLIENT confirms and ensures its compliance with Applicable Data Protection Law in its use of PROVIDER Services and confirms that its processing of Personal Data as specified under the Agreement and this DPA is lawful, fair, and transparent in relation to the Data Subjects.

3.2. The CLIENT shall be solely responsible for assessing whether Personal Data can be processed lawfully and for safeguarding the rights of the Data Subjects so that PROVIDER can provide the agreed PROVIDER Services in a way that does not violate any legal regulations, including Applicable Data Protection Law.

3.3. In particular, the CLIENT is responsible:

- for providing Data Subjects with a transparent privacy notice that meets the requirements of the Applicable Data Protection Law, including adequate notice of engaging PROVIDER as a processor, and
- for ensuring that the processing of Personal Data is based on the appropriate legal basis (for example, by collecting consents).

4. OBLIGATIONS OF PROVIDER

4.1. Permitted purposes

4.1.1. PROVIDER shall process Personal Data in the context of the concluded Agreement, only to the extent required, and in the appropriate way necessary to provide PROVIDER Services to the CLIENT under the Agreement.

4.2. Instructions

4.2.1. PROVIDER shall process Personal Data in accordance with the Agreement, this DPA, and Applicable Data Protection Law and only upon the documented instructions of the CLIENT, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so under mandatory law to which PROVIDER is subject. The CLIENT shall ensure that its instructions are lawful, and that PROVIDER's processing of Personal Data will not cause PROVIDER to violate any applicable law, regulation, or rule, including the Applicable Data Protection Law.

4.2.2. In the event that a mandatory law prevents PROVIDER from complying with such instructions or imposes a legal requirement on PROVIDER to process Personal Data, PROVIDER shall inform the CLIENT in writing of such a legal requirement before carrying out the relevant processing activities, unless PROVIDER is prohibited under that law from informing the CLIENT of such processing.

4.2.3. PROVIDER shall immediately inform the CLIENT if, in its opinion, an instruction infringes Applicable Data Protection Law. PROVIDER shall be entitled to suspend performance of such an instruction until it is clarified or changed by the CLIENT.

4.3. Confidentiality

4.3.1. PROVIDER shall treat all Personal Data as confidential and it shall ensure the reliability of all its employees, agents, and/or approved sub-processors engaged in the processing of Personal Data.

4.3.2. PROVIDER shall ensure that access to Personal Data is available only to those PROVIDER's employees and other persons operating on behalf of PROVIDER who are under confidentiality obligations with respect to Personal Data and who have received appropriate training.

4.4. Security of Personal Data

4.4.1. PROVIDER warrants that it maintains and shall continue to maintain adequate security measures (technical and organisational) to protect Personal Data against accidental loss, destruction, damage, alteration, unauthorized disclosure of, or access to, and against all other unlawful forms of processing, considering (i) the nature, scope, context, and purposes of the processing, (ii) risks posed to Data Subjects, (iii) the state-of-the-art, and (iv) implementation expenses, including, inter alia, as appropriate:

- the pseudonymisation and/or encryption of Personal Data when possible/appropriate;
- the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident;
- an established process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures;
- measures to identify vulnerabilities with regards to the processing of Personal Data in systems used to provide PROVIDER Services to the CLIENT;
- other reasonable security measures agreed upon by the Parties.

A specification of technical and organisational measures implemented by PROVIDER is available at https://www.infobip.com/assets/downloads/Technical_and_organisational_measures.pdf, and a list of certifications is available at https://www.infobip.com/certificates.

4.4.2. At the request of the CLIENT, PROVIDER shall demonstrate the measures it has taken pursuant to this Article, allowing the CLIENT to audit and test such measures in accordance with Article 4.7. of this DPA.

4.4.3. The CLIENT acknowledges that the PROVIDER Services include certain features and functionalities that PROVIDER requires or recommends, as a minimum standard, to the CLIENT to implement and use since those may impact the security of the data processed by the CLIENT's use of the PROVIDER Services, such as, encryption of communications content, availability of multi-factor authentication on the CLIENT's account, device fingerprinting, IP whitelisting, or usage of TLS encryption and secure file transfer protocol (SFTP). The list of security obligations and minimal recommendations, maintained by PROVIDER in accordance with applicable best practices, is available to the CLIENT at https://www.infobip.com/docs/essentials/security-recommendations. The CLIENT is responsible for properly configuring PROVIDER Services and using the available features and functionalities to maintain the appropriate level of security considering the nature of the data processed by the CLIENT in its use of PROVIDER Services. The CLIENT shall be held solely liable for any security incident or Personal Data Breach occurring as a result of not adhering to PROVIDER's recommended security measures.

4.4.4. The PROVIDER will perform the proper security activities to prevent and identify illicit use of CLIENT's account and PROVIDER's systems. The PROVIDER will notify the CLIENT when it detects a suspicious illicit activity affecting its account.

4.4.5. The Parties acknowledge that security requirements are constantly changing, and that effective security requires frequent evaluation of and regular improvements to outdated security measures. When necessary, PROVIDER therefore ensures it will tighten, supplement, and improve these measures in order to maintain compliance with the requirements set out in this DPA. The Parties will negotiate the cost in good faith, if there is any, to implement material changes required by specific updated security requirements set forth in the Applicable Data Protection Law or by the supervisory authorities of the competent jurisdiction.

4.4.6. Where an amendment to the Agreement is necessary in order to execute the CLIENT's instruction to PROVIDER to improve security measures, as may be required by changes in Applicable Data Protection Law from time to time, the Parties shall negotiate an amendment to the Agreement in good faith.

4.5. Responding to Data Subject and third-party requests

4.5.1. In the event that PROVIDER receives a request, complaint, enquiry, or communication from a Data Subject, supervisory authority, or third party (hereinafter: "**notifications**") which relates to the processing of Personal Data or to the CLIENT's compliance with the Applicable Data Protection Law or this DPA, PROVIDER will, where known by PROVIDER at the time of such notification, notify the CLIENT no later than within five (5) working days. Unless obliged to do so by mandatory laws, PROVIDER shall not respond to any such notification without the CLIENT's prior written consent, except to confirm that such a request relates to the CLIENT. PROVIDER will assist the CLIENT by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the CLIENT's obligations laid down in the Applicable Data Protection Law to respond to such notifications from Data Subjects.

4.6. Assistance with the CLIENT's compliance

4.6.1. Taking into account the nature of processing and the information available to PROVIDER, PROVIDER shall provide the CLIENT, insofar as this is possible and at the CLIENT's written request, with all information required for the CLIENT to comply with statutory obligations under Applicable Data Protection Law (in particular, the obligations necessary to ensure the CLIENT's compliance with security of processing, personal data breach notification, data protection impact assessment, and prior consultations with supervisory authorities), and will assist the CLIENT, insofar as reasonable, in meeting these statutory obligations.

4.7. Information and audit

4.7.1. CLIENT may request information related to PROVIDER's processing of Personal Data, if necessary to confirm PROVIDER's compliance with this DPA and Applicable Data Protection Law, in the form of a report or by conducting an audit as stipulated under conditions set out in point 14. (Compliance) of PROVIDER's Information security terms.

4.7.2. Notwithstanding the previous, the Parties agree that the CLIENT may require information on PROVIDER's compliance with this DPA and Applicable Data Protection Law when the CLIENT is expressly requested or required to provide such information to its supervisory authority, and it may conduct an audit at any time in the event of a confirmed Personal Data Breach.

4.8. Personal Data Breach notification

4.8.1. In the case of a Personal Data Breach as defined by Applicable Data Protection Law, and to the extent required by such Law, PROVIDER shall, without undue delay after having become aware of it, notify the CLIENT of the Personal Data Breach. PROVIDER shall cooperate with the CLIENT and shall make all reasonable efforts to identify and remediate the cause of such Personal Data Breach.

4.8.2. Such notification shall be sent to the CLIENT at the e-mail address, specified in Annex 1, and shall include, at the time of notification or as soon as possible after notification:

- the description of the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects concerned as well as the categories and estimated number of Personal Data records concerned;
- the name and contact details of the data protection officer or other contact point for further relevant inquiries;
- a description of the likely consequences of the Personal Data Breach;
- a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;
- any other information if mandatory under Applicable Data Protection Law.

4.8.3. The CLIENT, as the controller, is solely responsible and authorised to notify the relevant supervisory authorities, and if applicable, the Data Subjects, of the Personal Data Breach. Therefore, unless required by mandatory law, PROVIDER shall not disclose or publish any statement, communication, notice, press release, or report regarding a Personal Data Breach nor notify Data Subjects or supervisory authorities without the CLIENT's prior written consent.

4.9. Obligations under the US Privacy Law

4.9.1. PROVIDER confirms that the CLIENT's or CLIENT's Consumers' Personal Information are processed, retained, used, and disclosed only as is necessary to provide PROVIDER Services in accordance with the Business Purpose and to provide the same level of privacy protection as is required by the US Privacy Law, i.e., for PROVIDER's Business Purposes, and are not Sold or Shared to anyone.

4.9.2. PROVIDER will not Sell or Share Personal Data nor use, disclose, or retain Personal Data for: (i) any purposes outside of providing the PROVIDER Services; (ii) for its own commercial purposes; or (iii) outside of the direct business relationship between PROVIDER and CLIENT.

4.9.3. Regarding Consumer rights in the sense of US Privacy Law, the provision of Article 4.5. will correspondingly apply.

4.9.4. The sub-processors PROVIDER relies on when providing PROVIDER Services under the Agreement as stipulated in Article 5. of this DPA are Service Providers in the sense of US Privacy Law. With such Service Providers, appropriate data processing agreements are concluded and impose data protection obligations no less onerous than those contained in this DPA, to the extent applicable to the nature of the services they provide. All the obligations of PROVIDER arising from Article 5. of this DPA regarding sub-processors shall apply accordingly.

4.9.5. Capitalized terms used in the Article 4.9., such as (but not limited to), "Sell", "Sold", "Share", "Shared", "Personal Information", "Business Purpose", "Consumers" and "Service Provider" shall have the meaning as set forth in the US Privacy Law.

4.9.6. PROVIDER certifies that it understands the restrictions set forth in this DPA and will comply with them.

5. SUB-PROCESSORS

5.1. The CLIENT agrees that PROVIDER engages processors (sub-processors) already listed at https://www.infobip.com/policies/processors and authorizes PROVIDER to engage further processors (sub-processors) to carry out specific processing activities on behalf of the CLIENT, under the conditions that:

- PROVIDER maintains an up-to-date list of its sub-processors at https://www.infobip.com/policies/processors, and informs the CLIENT of any addition or replacement within the sub-processors list, providing the CLIENT with an opportunity to object to such changes. The Parties agree that the CLIENT will subscribe to notifications of changes within the sub-processors list, and

PROVIDER shall notify the CLIENT of any intended changes within the sub-processors list that affect the CLIENT at least 30 (thirty) calendar days before the change;

- The CLIENT has not objected to the change within the sub-processors list within the period of 30 (thirty) calendar days from having received PROVIDER's written notification, in which case it will be presumed that approval for the change has been obtained;

- PROVIDER has imposed on the sub-processor data protection obligations not less onerous than those contained in this DPA, to the extent applicable to the nature of the services provided by such sub-processor by way of a written contract or other legal act according to the Applicable Data Protection Law.

5.2. The CLIENT may object to the use of a new sub-processor where there are reasonable grounds to believe that the new sub-processor will be unable to comply with the Agreement/this DPA. The CLIENT acknowledges that the inability to use a particular new sub-processor may result in a delay in the performing of PROVIDER Services, in an inability to perform PROVIDER Services, or in increased fees. In such a case, the Parties will either execute a written amendment to the Agreement/this DPA or terminate the Agreement/this DPA under the terms of the Agreement, whereby neither Party shall be entitled to reimbursement or compensation from damages arising from, or resulting from, the termination under this Article.

5.3. Where the sub-processor engaged by PROVIDER fails to fulfil its data protection obligations, PROVIDER shall remain fully liable to the CLIENT for the performance of the sub-processor's obligations.

5.4. To the extent required by Applicable Data Protection Law, the CLIENT may request that PROVIDER audits the sub-processor or provides confirmation that such an audit has occurred to ensure compliance with its obligations arising from the contractual relationship as far as processing activities carried out on behalf of the CLIENT are concerned.

6. INTERNATIONAL DATA TRANSFERS

6.1. When processing under this DPA requires the international transfer of Personal Data, PROVIDER will comply with Applicable Data Protection Law, including, where necessary, the implementation of contractual mechanisms such as standard contractual clauses for data transfers.

6.2. Unless otherwise agreed with the CLIENT in writing (including e-mail), PROVIDER shall ensure that Personal Data are stored and processed at the processing systems located in its data centres within the European Union (EU) or European Economic Area (EEA), and any transfer of Personal Data to PROVIDER's data centres located outside the EU or EEA can be made only upon such an instruction by the CLIENT.

7. TERM AND TERMINATION, DELETION, AND RETURN OF PERSONAL DATA

7.1. This DPA shall come into effect upon the signature of both Parties and shall be valid for the duration of the actual provision of PROVIDER Services by PROVIDER.

7.2. The termination or expiration of this DPA shall not discharge PROVIDER from its confidentiality obligations pursuant to Article 4.3. of this DPA.

7.3. Should PROVIDER be in a material breach of any provision of this DPA, the CLIENT has the right to terminate both this DPA as well as the Agreement for cause, in whole or in part, under the conditions defined in the Agreement.

7.4. During the term of the Agreement and/or this DPA, the PROVIDER shall retain Personal Data following PROVIDER's data retention policy and schedule applicable to PROVIDER Services, unless otherwise agreed with the CLIENT. Upon termination of the Agreement and/or this DPA for any reason, and at the CLIENT's decision, Personal Data will be returned or deleted within thirty (30) days after the termination of this Agreement and/or the DPA. PROVIDER shall not retain any copies of Personal Data unless otherwise required or permitted by mandatory law..

8. MISCELLANEOUS

8.1. This DPA is an integral part of the Agreement. If there is a conflict between this DPA and the Agreement, the provisions of this DPA will prevail. For all questions not regulated under this DPA, the provisions of the Agreement shall prevail.

8.2. Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

9. ANNEXES

9.1. The following Annexes are integral parts of this DPA:

- Annex 1: Details about Personal Data processing
- Annex 2: Data Transfer Agreement (EU Standard Contractual Clauses and UK Addendum). When applicable, if and to the extent the Data Transfer Agreement conflicts with any provision of this DPA, the Data Transfer Agreement shall prevail.

For and on behalf of: Infobip

Signature Silvio Kutic
D41A86505D5F454...

Date: 19 January 2024
Name: Silvio Kutić
Position: Director

For and on behalf of: Client

Signature

Date:
Name:
Position: Director

ANNEX 1 – DETAILS ABOUT PERSONAL DATA PROCESSING

Nature and purposes of the processing:

The nature and purposes of the processing are defined in the Agreement.

The CLIENT, as the controller, commissions PROVIDER, as the processor, to process Personal Data for the following processing activities:

- Provision of business communication products and services through the cloud communication platform to the CLIENT, including transmission of communications from or to the CLIENT's software application (API) or via the PROVIDER's web-based interface (Customer Portal) towards telecom operators or other communication networks;
- Storage of the CLIENT's Personal Data on the PROVIDER's platform on behalf of the CLIENT;
- Reporting and analysis and handling other CLIENT's enquiries according to the CLIENT's instructions;
- Blocking communications to phone numbers based on risk score thresholds agreed with the CLIENT using Signals service.

Duration of the processing:

The processing of Personal Data shall be carried out during the provision of PROVIDER Services.

Categories of Data Subjects:

The Personal Data processed may generally concern the following Data Subjects: the CLIENT's customers or employees (all of them, hereinafter: „**end-users"**). In any case, and depending on the product/feature used, the precise categories of Data Subjects are always determined solely by the CLIENT.

Categories of Personal Data:

In any case, and depending on the product/feature used, the precise categories of Personal Data are always determined solely by the CLIENT.

Data category	Product/feature
CLIENT's communications content (text, voice, video and audio media, documents, images) and associated communication logs (e.g., timestamp and receiver/sender contact data such as MSISDN, land phone number, or email address)	Communication channels
CLIENT's databases stored on the PROVIDER's platform (*People*) with the CLIENT's end-users' data (such as name, contact details, birthday, and gender) imported by the CLIENT or collected on behalf of the CLIENT when providing PROVIDER Services	People
Personal data processed in Reports and analysis	All
Communication exchanged via contact center through Conversations product	Conversations
Communication exchanged via contact center through Answers product	Answers
Communication exchanged via contact center through Moments product	Moments
Logs about Live Chat users (such as the URL where a chat was started by an end-user, the IP-based location of the end-user session when he started a chat, browser/mobile device system information, timestamps)	Live Chat
CLIENT's databases stored in the PROVIDER Knowledge Base	Knowledge Base
Social Media data (end-users' social media ID, username, comment ID, post ID, content and timestamp of comments/posts, social media page ID)	Social Media
Resources provided by the CLIENT for AI analysis, communication exchanged via the Experiences product	Experiences

Special categories of Personal Data:

PROVIDER does not intentionally collect or process any special categories of Personal Data unless the CLIENT or its end-users include such types of data in the content submitted to PROVIDER and/or while using PROVIDER Services.

Contact details for data protection enquiries:

The CLIENT shall provide to PROVIDER the email address and other contact details for data protection enquiries, including Personal Data Breach notifications. If applicable, the CLIENT shall also provide name and contact details of the CLIENT's EU representative, in accordance with Article 27 of the GDPR.

The PROVIDER shall store the email address and other contact details of the CLIENT in its systems. Regardless of the foregoing, PROVIDER reserves the right to send Personal Data Breach notifications to the authorised user of the CLIENT's account (e.g., its related business contacts).

Contact details of PROVIDER:

E-mail: privacy@infobip.com

E-mail for personal data breach notifications: DataBreach@infobip.com

ANNEX 2 - DATA TRANSFER AGREEMENT

In light of the Parties' processing roles as defined in the DPA and the nature of international data transfer occurring during the provision of PROVIDER Services, the Parties agree that one of the following Data Transfer Agreements (hereinafter: "**DTA**“) may apply:

- DTA between the CLIENT established in the EU (the data exporter) and the PROVIDER established in the third country (the data importer)

  
  Modules 2+3.pdf

- DTA between the CLIENT established in the UK (the data exporter) and the PROVIDER established in the third country (the data importer)

  
  UK Addendum_Modules 2

- DTA between the PROVIDER established in the EU (the data exporter) and the CLIENT established in the third country (the data importer)

  
  Module 4.pdf

- DTA between the PROVIDER established in the UK (the data exporter) and the CLIENT established in the third country (the data importer)

  
  UK Addendum_Module 4