Once fully executed, this Data Processing Agreement forms a part of the Agreement between the PROVIDER and the COMPANY 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 COMPANY needs to:

1. Complete the information as the "COMPANY" on page 1
2. Complete the signature box and sign on page 7
3. Complete the contact details on page 9
4. 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 "COMPANY" 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 COMPANY (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 COMPANY, 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

1.1. For the purposes of this DPA, the following definitions apply:

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) **"CCPA"** shall mean the California Consumer Privacy Act of the 2018.

c) **"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 COMPANY as described in Annex 1.

d) **"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 COMPANY.

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 COMPANY 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 COMPANY

3.1. The COMPANY 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 COMPANY 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 COMPANY 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 COMPANY 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 COMPANY, 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 COMPANY 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 COMPANY in writing of such a legal requirement before carrying out the relevant processing activities, unless PROVIDER is prohibited under that law from informing the COMPANY of such processing.

4.2.3. PROVIDER shall immediately inform the COMPANY 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 COMPANY.

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 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 COMPANY;
- 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/company.

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

4.4.3. The COMPANY acknowledges that the PROVIDER Services include certain features and functionalities that INFOBIP requires as a minimum standard, for the COMPANY to implement and use since those may impact the security of the data processed by the COMPANY's use of the PROVIDER Services. The list of security rules and recommendations, maintained by PROVIDER in accordance with applicable best practices, is regularly updated and available to the COMPANY at https://www.infobip.com/docs/essentials/security-recommendations. The COMPANY is responsible for the proper configuration of configurable parameters and usage of the available features and functionalities to maintain the appropriate level of security considering the nature of the data processed through PROVIDER Services. In case the COMPANY chooses to apply weaker security measures than those recommended by PROVIDER, the COMPANY accepts related security risks and PROVIDER disclaims any liability for consequences that may arise from such usage

of PROVIDER's Services. In case the PROVIDER implements significant changes to the security measures, that would require any actions by the COMPANY, the COMPANY will be timely notified in advance through agreed communication channels.

4.4.4. 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.

4.4.5. Where an amendment to the Agreement is necessary in order to execute the COMPANY'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 COMPANY's compliance with the Applicable Data Protection Law or this DPA, PROVIDER will, to the extent legally permitted, immediately (and where known by PROVIDER at the time of such notification, no later than within five (5) working days), notify to the COMPANY any such notification received by PROVIDER. Unless obliged to do so by mandatory laws, PROVIDER shall not respond to any such notification without the COMPANY's prior written consent, except to confirm that such a request relates to the COMPANY. PROVIDER will assist the COMPANY by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the COMPANY's obligations laid down in the Applicable Data Protection Law to respond to such notifications from Data Subjects.

4.6. Assistance with the COMPANY's compliance

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

4.7. Information and audit

4.7.1. **Reports.** COMPANY acknowledges that PROVIDER is regularly audited against ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 and ISAE 3000 standards. Upon COMPANY's written request, PROVIDER will provide COMPANY with a full or summary copy, as applicable, of its then-current reports and certificates (hereinafter: **"Report"**). PROVIDER shall also provide, not later than ten (10) working days, written responses to all reasonable requests made by COMPANY for information relating to PROVIDER's processing of Personal Data, including responses to information, privacy and security audit questionnaires submitted by COMPANY and that are necessary to confirm PROVIDER's compliance with this DPA and Applicable Data Protection Law, provided that COMPANY shall not exercise this right more than once per year or when COMPANY is expressly requested or required to provide this information to a data protection authority.

4.7.2. **Audits.** While it is the Parties' intention to ordinarily rely on the Report and written responses described under Section 4.7.1. of this DPA to verify PROVIDER's compliance with this DPA and Applicable Data Protection Law, where so stipulated by applicable legislation and/or regulation, COMPANY may request PROVIDER, with thirty (30) days' prior written notice or shorter if so determined by such legislation/regulation, to conduct an audit of PROVIDER's records, reports, and information (hereinafter: **"Audit documentation"**) maintained by PROVIDER in relation to this DPA to ensure PROVIDER's compliance with the obligations as a processor, provided that: (i) the audit shall be conducted at COMPANY's expense; (ii) the Parties shall mutually agree upon the scope, timing and duration of the audit; and (iii) the audit shall not unreasonably impact PROVIDER's regular operations. PROVIDER shall cooperate and agrees to provide the COMPANY with access to Audit documentation maintained by PROVIDER reasonably required to conduct the audit. However, PROVIDER reserves the right to impose limitations or require additional assurances from the COMPANY as

may be necessary to protect confidential information of PROVIDER that may be accessed by the COMPANY as a part of any such audit.

4.7.3. Notwithstanding the foregoing, the Parties agree that the COMPANY may conduct an audit at any time in the event of a (i) confirmed Personal Data Breach, (ii) audits required by COMPANY's governmental or regulatory authorities, or (iii) investigations of claims of misappropriation, fraud, or business irregularities of a potentially criminal nature required by law enforcement and/or judicial bodies.

4.7.4. The COMPANY may perform the audits itself or have them performed by another auditor it has commissioned at its own expense, with the auditor being subject to PROVIDER's prior approval. Persons or third parties entrusted with such audits by the COMPANY must be obliged, in writing, to maintain confidentiality, and PROVIDER must be appropriately informed of their being commissioned.

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, immediately after having become aware of it, notify the COMPANY of the Personal Data Breach. PROVIDER shall cooperate with the COMPANY 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 COMPANY 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 COMPANY, 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 COMPANY's prior written consent.

4.9. Obligations under the CCPA

4.9.1. PROVIDER confirms that the COMPANY's or COMPANY's Consumers' Personal Information are processed, retained, used, and disclosed only as is necessary to provide PROVIDER Services, i.e., for PROVIDER's business purposes, and are not sold to anyone.

4.9.2. Regarding Consumer rights in the sense of CCPA, the provision of Article 4.5. will correspondingly apply.

4.9.3. 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 CCPA. 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.

4.9.4. Capitalized terms used in this Article 4.9. shall have the meaning set forth in the CCPA. For clarity, the terms used in this DPA, such as (but not limited to) „Personal Data", „Data Subjects" and „Processor" include "Personal Information", "Consumers" and "Service Provider" respectively, as defined under CCPA.

5. SUB-PROCESSORS

5.1. The COMPANY authorizes PROVIDER to engage further processors (sub-processors) to carry out specific processing activities on behalf of the COMPANY, 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 COMPANY of any addition or replacement within the sub-processors' list, providing the COMPANY with an opportunity to object to such changes. The Parties agree that the COMPANY will subscribe to notifications of changes within the sub-processors' list, and PROVIDER shall notify the COMPANY of any intended changes within the sub-processors' list that affect the COMPANY at least 30 (thirty) calendar days before the change;

- The COMPANY 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 COMPANY 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 COMPANY 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 COMPANY for the performance of the sub-processor's obligations.

5.4. To the extent required by Applicable Data Protection Law, the COMPANY 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 COMPANY 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 COMPANY 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 COMPANY.

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.

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, COMPANY 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. Upon termination of the Agreement and/or this DPA for any reason, and at the decision of the COMPANY, Personal Data will be returned or deleted within thirty (30) days as of the termination of this Agreement and/or the DPA. PROVIDER shall not retain any copies of Personal Data unless otherwise required 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.

8.3. This DPA is made and entered into as of the Effective Date. The Effective Date of this DPA shall be the date of last signature set forth below. This DPA shall not be effective until both Parties have signed.

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 (only if applicable)

For and on behalf of: Infobip	**For and on behalf of: Company**
Signature DocuSigned by: Silvio Kutic D41A86505D5F454...	*Signature*_____
Date: 21.09.2022.	Date:
Name: Silvio Kutic	Name:
Position: Director	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 COMPANY, as the controller, commissions to PROVIDER, as the processor, Personal Data processing for the following processing activities:

- Provision of business communication products and services through the cloud communication platform on behalf of the COMPANY, including transmission of communications from or to the COMPANY's software application (API) or via the PROVIDER web-based interface (Customer Portal) towards telecom operators or other communication networks;
- Storage of the COMPANY's Data on the PROVIDER platform on behalf of the COMPANY;
- Reporting and analysis and handling other COMPANY's enquiries according to the COMPANY's instructions.

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 COMPANY'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 COMPANY.

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 COMPANY.

	Data category	Product/feature
	COMPANY's communications content (text, voice, video and audio media, documents, images) and associated communication logs, (to the extent they contain Personal Data)	Communication channels
	Reports and analysis (to the extent they contain Personal Data)	All
	COMPANY's databases stored on PROVIDER platform with COMPANY's end-users' Personal Data, i.e. name, contact details, and any other information defined, imported, and controlled exclusively by the COMPANY, or collected on behalf of the COMPANY when providing PROVIDER Services	People
	Communication exchanged via contact center through Conversations product (to the extent they contain Personal Data)	Conversations
	Communication exchanged via contact center through Answers product (to the extent they contain Personal Data)	Answers
	Communication exchanged via contact center through Moments product (to the extent they contain Personal Data)	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
	COMPANY's databases stored in the PROVIDER Knowledge Base (to the extent they contain Personal Data)	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

Special categories of Personal Data:PROVIDER does not intentionally collect or process any special categories of Personal Data unless the COMPANY 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:

Contact details of the COMPANY:

E-mail for general data protection matters:

E-mail for Personal Data Breach notifications:
In any case, PROVIDER reserves the right to send Personal Data Breach notifications to the authorised user of the COMPANY's account (e.g., its related business contacts).

Name and contact details of the COMPANY's representative, if applicable
(only for COMPANYS established outside the EU, if the COMPANY is obliged to designate a representative in the EU in accordance with Article 27 of the GDPR)

Name:
Address:
E-mail:

E-mail for Personal Data Breach notifications:
In any case, PROVIDER reserves the right to send Personal Data Breach notifications to the authorised user of the COMPANY's account (e.g., its related business contacts).

Contact details of PROVIDER:

E-mail for general data protection matters: Corporate_Privacy@infobip.com

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

ANNEX 2: DATA TRANSFER AGREEMENT

This **Data Transfer Agreement** (hereinafter: DTA) is made and entered into between PROVIDER, hereinafter referred to as "Infobip" or "**data exporter**" and COMPANY, hereinafter referred to as "**data importer**" and together with Infobip, the "Parties".

INTRODUCTION

Whereas

a) The Parties have entered into one or more agreements (hereinafter: **"Main Agreement"**) that require the processing of personal data;

b) In the course of the processing of personal data as defined in the Main Agreement it is necessary for Infobip to transfer, as data exporter, personal data to the Company, as data importer;

c) The European Commission adopted the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council [2021] OJ L199/31 (hereinafter: EU Standard Contractual Clauses);

d) The United Kingdom's Information Commissioner issued the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses under S119A(1) of the Data Protection Act (hereinafter: UK Addendum);

Now therefore, the Parties agree as follows:

1. This DTA is made and entered into as of the Effective Date. The Effective Date of this DTA shall be the Effective Date of the DPA.

2. If and when the data exporter's and data importer's country of origin reach an adequacy regulation, this DTA will cease to be in effect from the day the adequacy regulation enters into force.

3. This DTA is an addendum to the Main Agreement. All other original terms and conditions of the Main Agreement shall remain unchanged and in full force and effect. For all questions not regulated under this DTA, the provisions of the Main Agreement shall apply.

4. The Parties have agreed to the terms of this DTA, to repeal the EU's Standard Contractual Clauses for international data transfers that were in place before this DTA entered into force, and implement its provisions with regard to the international data transfers subject to the European Union's data protection laws in the manner as set forth below.

A. EU Standard Contractual Clauses

1. The EU Standard Contractual Clauses are hereby incorporated into this Data Transfer Agreement by this reference.

2. The Parties will apply the **Module Four** of the EU Standard Contractual Clauses to international transfers of personal data carried out by any Infobip subsidiary or affiliate located in the European Union, acting as data exporter, to the Company, located in a third country for which the European Commission did not issue a decision on adequate level of personal data protection.

3. To implement the EU Standard Contractual Clauses the Parties agree:

   a. Not to apply the optional docking clause in Clause 7;
   b. Not to apply the Option in Clause 11;

B. UK Addendum

1. The UK Addendum is applied only to international transfers of personal data carried out by Infobip or any Infobip subsidiary or affiliate located in the United Kingdom, acting as data exporter, to the Company, located in a third country for which the United Kingdom did not issue a decision on adequate level of personal data protection, as follows:

1.1 ***International Data Transfer Addendum to the EU Commission Standard Contractual Clauses***
VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

1.2 Part 1: Tables
1.2.1 Table 1: Parties

Start date	*Date of signature of this Data Transfer Agreement*	
The Parties	***Exporter (who sends the Restricted Transfer): Infobip***	***Importer (who receives the Restricted Transfer): Company***
Parties' details	*Indicated in Section D of the Data Transfer Agreement*	*Indicated in Section D of the Data Transfer Agreement*
Key Contact	*Indicated in Section D of the Data Transfer Agreement*	*Indicated in Section D of the Data Transfer Agreement*

1.2.2 Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		X The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	N/A	N/A	N/A			
2	N/A	N/A	N/A	N/A	N/A	
3	N/A	N/A	N/A	N/A	N/A	
4	X	N/A	N/A			N/A

1.2.3 Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Annex Section A to the Data Transfer Agreement

Annex 1B: Description of Transfer: Annex Section B to the Data Transfer Agreement

1.2.4 Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: X Importer X Exporter

1.3 Part 2: Mandatory Clauses

1.3.1 Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

1.3.2 Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.

Appendix Information	*As set out in Table 3.*
Appropriate Safeguards	*The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.*
Approved Addendum	*The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.*
Approved EU SCCs	*The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.*
ICO	*The Information Commissioner.*
Restricted Transfer	*A transfer which is covered by Chapter V of the UK GDPR.*
UK	*The United Kingdom of Great Britain and Northern Ireland.*
UK Data Protection Laws	*All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.*
UK GDPR	*As defined in section 3 of the Data Protection Act 2018.*

4. *This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.*

5. *If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.*

6. *If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.*

7. *If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.*

8. *Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.*

1.3.3 Hierarchy

9. *Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.*

10. *Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.*

11. *Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.*

1.3.4 Incorporation of and changes to the EU SCCs

12. *This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:*

a. *together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;*

b. *Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and*

c. *this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.*

13. *Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.*

14. *No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.*

15. *The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:*

a. *References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;*

b. *In Clause 2, delete the words:*

> *"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";*

c. *Clause 6 (Description of the transfer(s)) is replaced with:*

> *"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";*

d. *Clause 8.7(i) of Module 1 is replaced with:*

> *"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";*

e. *Clause 8.8(i) of Modules 2 and 3 is replaced with:*

> *"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"*

f. *References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;*

g. *References to Regulation (EU) 2018/1725 are removed;*

h. *References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";*

i. *The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";*

j. *Clause 13(a) and Part C of Annex I are not used;*

k. *The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";*

l. *In Clause 16(e), subsection (i) is replaced with:*

> *"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";*

m. *Clause 17 is replaced with:*

> *"These Clauses are governed by the laws of England and Wales.";*

n. *Clause 18 is replaced with:*

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. *The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.*

1.3.5 Amendments to this Addendum

16. *The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.*

17. *If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.*

18. *From time to time, the ICO may issue a revised Approved Addendum which:*

    a. *makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or*
    b. *reflects changes to UK Data Protection Laws;*

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. *If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:*
    a *its direct costs of performing its obligations under the Addendum; and/or*
    b *its risk under the Addendum,*
    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. *The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.*

1.4 Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	*Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.*

C. ANNEX

1. List of Parties

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]: ***Indicated in Section D of the data Transfer Agreement.***

Activities relevant to the data transferred under these Clauses: ***Provision of data exporter's services to the data importer as described in the agreements for Infobip services between the parties.***

Signature and date: ***Indicated in the signature chart of this Data Transfer Agreement.***

Role (controller/processor): ***Processor***

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]: ***Indicated in Section D of the Data Transfer Agreement.***

Activities relevant to the data transferred under these Clauses: ***Provision of data exporter's services to the data importer as described in the agreements for Infobip services between the parties.***

Signature and date: ***Indicated in the signature chart of this Data Transfer Agreement.***

Role (controller/processor): ***Controller***

2. Description of transfer

Categories of data subjects whose personal data is transferred: ***The same as described in the agreement signed between the data exporter and data importer in accordance with Art. 28 of the GDPR (data processing agreement).***

Categories of personal data transferred: ***The same as described in the agreement signed between the data exporter and data importer in accordance with Art. 28 of the GDPR (data processing agreement).***

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: ***Non-applicable.***

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): ***Continuous basis.***

Nature of the processing and purpose(s) of the data transfer and further processing: ***The same as described in the agreement signed between the data exporter and data importer in accordance with Art. 28 of the GDPR (data processing agreement).***

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: ***Non-applicable.***

D. DETAILS OF THE PARTIES

The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Details of the Parties are specified in the Data Processing Agreement and the Data Transfer Agreement.	Details of the Parties are specified in the Data Processing Agreement and the Data Transfer Agreement.
Key Contact	Contact details of the Parties are listed in the Data Processing Agreement and the Data Transfer Agreement.	Contact details of the Parties are listed in the Data Processing Agreement and the Data Transfer Agreement.