DATA PROCESSING AGREEMENT

Route Mobile Limited

POLICY EFFECTIVE FROM JANUARY 01, 2026

VERSION 1.0

LAST UPDATED JANUARY 01, 2026

Contents

Preamble

This Data Processing Agreement ("Agreement") governs the processing of Personal Data by Route Mobile Limited and its affiliates (collectively, "Route Mobile", "we", or "us") in connection with the services it provides to its customers ("Customer", "you"), hereinafter collectively referred to as “Parties” and individually “Party”.

This DPA is effective as of the date Customer first uses the Services after the "Last Updated" date stated above and remains in effect for as long as Route Mobile processes Personal Data on your behalf.

This Agreement shall govern and be applicable to all exchanges of Personal Data between the Parties. Route Mobile is referred to as “Processor”, while the Customer is referred to as “Controller” or “Data Fiduciary”.

WHEREAS:

1. The Parties have entered into a Master Service Agreement (hereinafter the “MSA”) for the provision of certain digital communication and customer engagement services (as further detailed in Annex I of the MSA) to and for each other, in the performance of which, the Processing of certain Personal Data provided by the Data Controller or by the Processor is necessary. By using our services, you agree to the terms of this Agreement, which supplements and forms an integral part of the MSA between Route Mobile and the Company, and it is a part of the contractual relationship entered into with the Processor.
2. "Data Protection Laws" means all applicable laws and regulations relating to the protection of Personal Data, including, but not limited to, the European Union's General Data Protection Regulation (GDPR), India’s Digital Personal Data Protection Act 2023 and its rules, Information Technology Act 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, any national implementing laws, regulations, and secondary legislation, as amended or updated from time to time, and any successor legislation to the GDPR, as well as any other applicable data protection or privacy legislation in the relevant jurisdiction. For the purposes of this Agreement, capitalized terms not otherwise defined herein shall have the meaning assigned in applicable Data Protection Laws.
3. Both Parties shall comply with their respective obligations, whether as a Controller or Processor, under applicable Data Protection Laws in relation to any processing of Personal Data in connection with the MSA. Neither Party shall knowingly engage in any act or omission that may result in a breach by itself or by the other Party of any applicable Data Protection Laws. This Data Processing Agreement governs the Processing of Personal Data provided to the Processor by the Controller in connection with the provision of the Services defined in the MSA.
4. The Processor (and any Sub-Processors it engages) shall process Personal Data in strict compliance with the terms of this DPA, the Controller's instructions, and applicable Data Protection Laws, taking into account the nature, purpose, duration, scope, context, and complexity of the Processing, as well as the type of Personal Data and categories of Data Subjects involved. The obligations set forth in this DPA and in Annex 1 hereto shall apply to all Processing activities performed by the Processor and its Sub-Processors.
5. Controller has determined that Processor is willing and is able to deliver the required services in compliance with Data Protection Laws,
6. In the course of the performance of its services Processor processes Personal Data on behalf of the Controller,
7. This Data Processing Agreement (DPA) is to be considered as Data Processing Agreement stipulated in Article 28 of the GDPR and other applicable Data Protection Laws,
8. The Parties further agree and acknowledge that for the purposes of this Agreement, the following terms shall be defined as follows:
    a. “Personal Data” is any information relating to an identified or identifiable natural person (a “Data Subject”). An identifiable natural person is one who can be identified, directly or indirectly, by an identifier such as a name, identification

number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

b. "Personal Data Breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
c. "Processing" is any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
d. "Data Subject" is the identified or identifiable natural person to whom Personal Data relates.
e. "Controller" or "Data Fiduciary" is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
f. "Processor" is a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.
g. "Sub-Processor" is a natural or legal person, public authority, agency or other body that assists a Processor in rendering services to a third-Party. The Party assisting the Processor shall be deemed the Sub-Processor.

having regard to the fact that,

- The Controller has access to the Personal Data of various Data Subjects,
- The Controller wants the Processor to execute certain types of processing in accordance with the services Agreement entered for the provision of the Services defined in said Agreement by the Processor to Controller
- The Controller has determined the purpose of and the means for the processing of Personal Data as governed by the terms and conditions referred to herein;
- The Processor has undertaken to comply with this data processing Agreement and to abide by the security obligations and all other aspects of the Data Protection Laws.
- The Controller is hereby deemed to be the responsible Party within the meaning of Article 5(2) of the GDPR and;
- The Processor is hereby deemed to be the Processor within the meaning of Article 4(8) of the GDPR;
- The Parties, having regard also to the provisions of Data Protection Laws, wish to lay down their rights and duties in writing in this Data Processing Agreement,

Parties hereby agree as follows:

1. Processor's obligations

1.1 The Processor undertakes to process Personal Data on behalf of the Controller in accordance with the conditions laid down in this Data Processing Agreement. The processing will be executed exclusively within the framework of the Agreement, and for all such purposes as may be agreed to subsequently.

1.2 The Processor shall refrain from making use of the Personal Data for any purpose other than as specified by the Controller. The Controller will inform the Processor of any such purposes which are not contemplated in this Data Processing Agreement.

1.3 The Processor shall warrant compliance with the applicable Data Protection Laws, such as the GDPR.

1.4 The Processor shall furnish the Controller promptly on request with details regarding the measures it has adopted to comply with its obligations under this Data Processing Agreement and the applicable Data Protection Laws.

1.5 The Processor's obligations arising under the terms of this Data Processing Agreement apply also to whomsoever processes Personal Data under the Processor's instructions.

1.6 The Processor warrants that it will only process the Personal Data in such manner as and to the extent it is necessary for the performance of the services under the signed MSA between the Parties, except where specifically instructed by the Controller, or for legitimate business purposes such as billing, account management, financial and internal reporting, combatting and preventing security threats, cyber-attacks, business modelling, prevention of fraud or spam, or to comply with a legal obligation to which the Processor is a subject, in which case the Processor will notify the controller of such legal obligations, unless the notification is prohibited due to public interest.

1.7 Processor will immediately inform the controller in writing (including e-mail), if Processor is of the opinion that an instruction of controller is in violation of, or causes a breach to applicable legislations including the GDPR.

1.8 The Processor shall, to the extent required by applicable Data Protection Laws, provide reasonable assistance to the Controller with:
(i) conducting data protection impact assessments (DPIAs),
(ii) consulting with competent supervisory authorities prior to processing where required, and
(iii) complying with the Controller's obligations under Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to the Processor.

1.9 In case of termination of this Agreement, or upon controller's written request, the Processor shall, either destroy or return the Personal Data to the controller in the manner prescribed by the controller. No copies of Personal Data will be retained by the Processor unless required by law.

1.10 In case of termination of this Agreement, the Processor shall notify all third Parties involved with the processing of the Personal Data of the termination of the Agreement and shall ensure that all such third Parties shall either destroy or return the Personal Data as requested by the controller.

1.11 The Processor shall take no unilateral decisions regarding the processing of the Personal Data for other purposes, including decisions regarding the provision thereof to third Parties and the storage duration of the data.

1.12 The Processor shall promptly inform the Controller if, in its opinion, an instruction infringes on the GDPR or any other relevant data protection provisions.

1.13 For the purposes of a Reseller MSA, all references to 'Customer' shall be interpreted to mean the Reseller Partner under this Agreement. The DPA governs Route Mobile's processing of Personal Data provided by the Reseller Partner, including Personal Data originating from its customers and their end users to the extent such data is processed in connection with the services provided under the MSA.

2. Controller's obligations

2.1 The Controller shall be solely responsible for determining the permissibility and lawfulness of the Personal Data it provides to the Processor for Processing, including the preservation of the rights of the relevant Data Subjects. As such, the Controller is responsible and expressly warrants that it shall demonstrably obtain the necessary and desirable consent of the relevant Data Subject (if applicable), which shall in any event include the right of the Personal Data of the relevant Data Subject to be forwarded to and Processed by the Processor.

2.2 The Controller shall ensure that its instructions, upon which the Processor shall process Personal Data, are lawful, such that the Processor's Processing of Personal Data for the provision of the Service will not cause the Processor to violate any applicable law, regulation or rule, including any applicable Data Protection Laws.

3. Transmission of personal data

3.1 The Processor may process the Personal Data in countries outside the European Union. In addition, the Processor may also transfer the Personal Data to a country outside the European Union provided that such country guarantees an adequate level of protection and it satisfies the other obligations applicable to it pursuant to this Data Processing Agreement and the applicable Data Protection Laws.

3.2 Upon request, the Processor shall notify the Controller as to which country or countries the Personal Data will be processed in.

3.3 The Processor shall ensure compliance with the GDPR and other applicable Data Protection Laws while processing Personal Data in third countries outside the EU, including adherence to the EU Standard Contractual Clauses (adopted on 4 June 2021 by the European Commission). The Processor shall promptly implement any updates to the EU SCCs as required by the European Commission or other competent supervisory authorities. The applicability of the relevant module of the EU SCCs will be determined based on the precise nature of the relationship between the two Parties involved in the data transfer, be it controller-to-controller, controller-to-Processor, or Processor-to-Sub Processor.

3.4 In case Personal Data is transferred between the Parties (whether as Data Exporter or Data Importer), and at least one Party is established in a country outside the EEA, the United Kingdom, or Switzerland not considered by the European Commission, the UK Secretary of State, or the Swiss Federal Council (as applicable) to have an adequate level of data protection, the Parties hereby agree that the applicable data transfer mechanism shall be incorporated into this DPA as follows:

3.4.1 For transfers subject to EU GDPR: The EU Standard Contractual Clauses (pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries) shall apply. The specific Module of the EU SCCs shall be determined by the respective roles of the Parties in relation to the Personal Data transferred, as further described in Annex 1 hereto.

3.4.1.1 If Module One (Controller to Controller) applies: In Clause 7, the optional docking clause will apply; in Clause 11, the optional language will not apply; in Clause 17, Option 1 will apply, and the EU SCCs will be governed as set by Article 13 of this DPA; in Clause 18(b), disputes shall be resolved before the courts of the country where the contracting Route Mobile entity is located; in case of doubt, Article 13 of this DPA applies.

3.4.1.2 If Module Two (Controller to Processor) applies: In Clause 7, the optional docking clause will apply; in Clause 9, Option 1 will apply, and the time period for prior notice of Sub-Processor changes shall be as set in Article 6 of this DPA; in Clause 11, the optional language will not apply; in Clause 17, Option 1 will apply, and the EU SCCs will be governed as set by Article 13 of this DPA; in Clause 18(b), disputes shall be resolved before the courts of the country where the contracting Route Mobile entity is located; in case of doubt, Article 13 of this DPA applies.

3.4.1.3 If Module Three (Processor to Processor) applies: In Clause 7, the optional docking clause will apply; in Clause 9, Option 1 will apply, and the time period for prior notice of Sub-Processor changes shall be as set in Article 6 of this DPA; in Clause 11, the optional language will not apply; in Clause 17, Option 1 will apply, and the EU SCCs will be governed as set by Article 13 of this DPA; in Clause 18(b), disputes shall be resolved before the courts of the country where the contracting Route Mobile entity is located; in case of doubt, Article 13 of this DPA applies.

3.4.2 Annex I of the EU SCCs shall be deemed completed with the information set out in the Preamble of this DPA; Annex II of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this DPA (Data Processing Description). The competent supervisory authority will be determined in accordance with the Applicable Data Protection Law; the information required for Annex III and IV is in the annexes to this DPA (technical and organizational measures and list of Sub-Processors).

3.4.3 For transfers subject to UK GDPR: Where a transfer of Personal Data is protected by the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0, in force 21 March 2022) issued by the Information Commissioner's Office ("UK Addendum") shall apply. The UK Addendum shall be deemed completed as follows: The EU SCCs (completed as set out in Clause (a) above) shall also apply to transfers of such Data; Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, as completed above; and the option "neither Party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the effective date of this DPA.

3.4.4 For transfers subject to Swiss DPA: In relation to Personal Data protected by the Swiss Federal Act on Data Protection ("Swiss DPA"), the EU SCCs (as incorporated and completed in accordance with Clause (a) above) will apply provided that: (i) references in the EU SCCs to "Regulation (EU) 2016/679" or the "GDPR" shall be interpreted as

references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" shall be interpreted as references to Switzerland and to Swiss law, as the case may be; (iii) the term 'member state' shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland); (iv) the EU SCCs should be interpreted as protecting the data of legal entities until the entry into force of the revised Swiss DPA, if applicable; (v) references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner (FDPIC) and competent courts in Switzerland; and (vi) if the Restricted Transfer is subject to both the Swiss DPA and the GDPR, then a parallel supervision takes place: FDPIC, insofar as the data Restricted Transfer is governed by the Swiss DPA; and the competent EU supervisory authority insofar as the Restricted Transfer is governed by the GDPR (the criteria of Clause 13(a) of the EU SCCs for the selection of the competent authority must be observed).

3.5 In the event of any conflict or inconsistency between the provisions of this Data Processing Agreement and the EU Standard Contractual Clauses or UK Addendum (as applicable), the provisions of the EU Standard Contractual Clauses or UK Addendum (as applicable) shall take precedence and control.

3.6 In the event that the EU Standard Contractual Clauses or any equivalent mechanism for international transfers are amended, invalidated, or replaced, the Parties agree to cooperate in good faith to implement an alternative lawful data transfer mechanism.

4. Allocation of responsibility

4.1 The Processor shall process Personal Data solely on behalf of and in accordance with the Controller's documented instructions, and under the ultimate responsibility of the Controller.

4.2 The Processor shall not be responsible for any processing of Personal Data that falls outside the scope of this Agreement, including but not limited to processing for purposes not communicated by the Controller, unauthorized processing by third Parties, or processing for purposes other than those specified by the Controller.

4.3 The Controller represents and warrants that it has a valid legal basis, including where required the express consent of Data Subjects, to process the Personal Data in accordance with applicable Data Protection Laws. The Controller further represents and warrants that the content and use of the Personal Data do not violate any applicable law or infringe upon the rights of any third Party.

5. Engaging of sub-processors

5.1 The Processor is authorised within the framework of the Agreement to engage Sub-Processors that are necessary for the Processor to perform the services in accordance with the Agreement, provided that all data protection obligations listed in this Agreement are met. The Parties acknowledge that engaging Sub-Processors is necessary for the performance of the services and that due to the nature of telecommunications services all or any such carrier engaged by the Processor for merely transmitting messages as a conduit in the telecommunications networks cannot be communicated to the Controller.

5.2 The Processor shall in any event ensure that such third Parties will be obliged to agree in writing to the same duties that are agreed between the Controller and the Processor.

5.3 The Processor shall notify Controller at least thirty (30) days in advance of any intended addition or replacement of Sub-Processors. Controller may object in writing to any new Sub-Processor on reasonable grounds relating to data protection within fifteen (15) days of such notice. If the Controller does not object within this period, the Sub-Processor will be deemed approved.

6. Duty to report

6.1 In the event of a Personal Data Breach, the Processor shall notify the Controller without undue delay and, where feasible, not later than seventy-two (72) hours after becoming aware of a Personal Data Breach, after which the Controller shall determine whether to inform the Data Subjects and/or the relevant regulatory authority(ies). This duty to report

applies irrespective of the impact of the breach. The Processor will endeavour that the furnished information is complete, correct and accurate.

6.2 If required by law and/or regulation, the Processor shall cooperate in notifying the relevant authorities and/or Data Subjects. The Controller remains the Party responsible for any statutory obligations in respect thereof.

6.3 The duty to report includes in any event the duty to report the fact that a breach has occurred, including details regarding:

- the (suspected) cause of the breach;
- the (currently known and/or anticipated) consequences thereof;
- the (proposed) solution;
- the measures that have already been taken.

6.4 The Processor shall assist the Controller in fulfilling its obligations related to the notification of Personal Data Breaches to the competent supervisory authorities and the affected Data Subjects, taking into account the nature of the processing and the information available to the Processor.

7. Security

7.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity of the rights and freedom of natural persons, the Processor shall implement reasonable technical and organisational measures to ensure a level of security appropriate for the risk, in particular the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the Personal Data transmitted, stored or otherwise processed, and comply with the security requirements contained in the Processor's Information Security policies based on ISO 27001. This includes, but is not limited to:

7.1.1 the Pseudonymisation and encryption of Personal Data;

7.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

7.1.3 the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

7.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

7.2 The Controller will only make the Personal Data available to the Processor if it is assured that the necessary security measures have been taken.

7.3 The Processor shall periodically review and update its security measures to ensure ongoing effectiveness and alignment with industry best practices.

8. Handling requests from involved parties

8.1 Where a Data Subject submits a request to the Processor to, for example, access, inspect, or to improve, add to, change or protect their Personal Data, the Processor will forward the request to the Controller and the request will then be dealt with by the Controller. The Processor may notify the Data Subject hereof.

8.2 The Processor shall assist the Controller in fulfilling its obligations to respond to Data Subject requests, taking into account the nature of the processing and the information available to the Processor.

9. Non disclosure and confidentiality

9.1 All Personal Data received by the Processor from the Controller and/or compiled by the Processor within the framework of this Agreement is subject to a duty of confidentiality vis-à-vis third Parties.

9.2 This duty of confidentiality will not apply in the event that the Controller has expressly authorised the furnishing of such information to third Parties, where the furnishing of the information to third Parties is reasonably necessary in view of the nature of the services instructions and the implementation of the MSA or this Agreement, or if there is a legal obligation to make the information available to a third Party.

10. Audit

10.1 In order to confirm compliance with this Agreement, the Controller shall be at liberty to conduct an audit by assigning an independent third Party who shall be obliged to observe confidentiality in this regard. Any such audit will follow the Processor's reasonable security requirements and will not interfere unreasonably with the Processor's business activities.

10.2 Audits may be conducted no more than once annually, with ninety (90) days prior written notice to the Processor unless required by applicable Data Protection Law or following a confirmed data incident.

10.3 The audit may only be undertaken when there are specific grounds for suspecting the misuse of Personal Data, and no earlier than two weeks after the Controller has provided written notice to the Processor.

10.4 The findings in respect of the performed audit will be discussed and evaluated by the Parties and, where applicable, implemented accordingly as the case may be by one of the Parties or jointly by both Parties.

10.5 The costs of the audit will be borne by the Controller.

11. Duration and termination

11.1 The Agreement may not be terminated in the interim unless the main MSA between Parties itself is terminated.

11.2 This Agreement may only be amended by the Parties subject to mutual consent.

11.3 The Processor shall provide its full cooperation in amending and adjusting this Agreement in the event of new privacy legislation.

11.4 Termination or expiration of this Agreement shall not discharge the Processor from its obligations meant to survive the termination or expiration of this Agreement.

12. Liability and indemnity

The Processor acknowledges that the obligations set forth in this DPA are essential and that any violation thereof may seriously harm the Customer. The Processor shall have full and sole liability for all damages resulting from a failure on its part to comply with the provisions of this DPA. Should any Data Subject to whom the Personal Data relates, a Supervisory Authority, a Data Protection Board, a court or any other regulatory body lodge a claim for compensation against the Customer that results from Processor's breach of its obligations under the Applicable Data Protection Law (a "Claim"), Processor shall assist and intervene in the Customer's defence against such Claim upon the Customer's request and shall indemnify and hold harmless the Customer against all costs and damages resulting from such Claim. The Controller shall give Processor prompt written notice of any such Claim and shall provide all reasonable cooperation in the defence and settlement of such Claim, at Processor's expense. The Customer shall not make any admission as to Processor's liability in respect of such a Claim and shall not agree to any settlement in respect of such a Claim without Processor's written consent.

13. Miscellaneous

13.1 The Data Processing Agreement and the implementation thereof will be governed by the law of the country in which the Processor is established.

13.2 Any dispute arising between the Parties in connection with and/or arising from this Data Processing Agreement will be referred to the competent court in the district where the Processor has its registered office.

13.3 In the case of any inconsistency between documents and the appendices thereto, the following order of priority will apply:

- the MSA or Agreement;
- this Data Processing Agreement;
- additional conditions, where applicable.

14. Contact us

If you have any questions about this DPA, please contact us at dpo@routemobile.com.

ANNEX I - Data Processing Details

Products and services offered by Route Mobile

#	Name of the Service	Brief Description of the Service	Categories of Personal DataProcessed	Categories of Data Subjects Affected
1	SendClean (Email Messaging)	A service that enables businesses to send and receive emails for marketing, transactional, and communication purposes.	-First and last name -Email address -IP address -Cookies for tracking -Content of the e-mail	-Customers' end users -Employees -Business partners -Marketing leads
2	RCS Business Messaging	Rich Communication Services (RCS) is an advanced messaging service offering features like branded sender IDs, rich media, scrollable carousels, quick replies, and CTA buttons for an interactive user experience.	- Phone number - Name - Device information (for RCS compatibility) - Message content (including rich media) - Read receipts and interaction data	- Customers' end users - Marketing leads
3	WhatsApp Business Platform	Enables businesses to communicate with their customers on the WhatsApp platform for notifications, customer service, WhatsApp calling, and marketing. Route Mobile provides this service and has enabled WhatsApp-based solution for various services.	- Phone number - Name - Profile picture - Message content (including rich media) - Read receipts and interaction data	- Customers' end users - Service users (e.g., metro commuters)
4	Viber Business Messages	Allows businesses to engage with customers through Viber, offering a channel for promotional messages, transactional alerts, and customer support. This is part of Route Mobile's Enhanced Business Messaging Solutions.	- Phone number - Name - Viber user ID - Message content (including rich media) - Interaction data	- Customers' end users - Marketing leads
5	Telegram for Business	An API-based service that allows businesses to use the Telegram messaging platform for customer communication, including sending notifications, providing customer support, and engaging with users through automated chatbots.	- Telegram user ID - Phone number (if provided by the user) - User's name and username - Message content and media files - Interaction metadata (e.g., read receipts)	- Customers' end users - Marketing leads - Users interacting with the business on Telegram
6	Truecaller Verified Business Identity Solutions	A partnership service enabling businesses to register and manage a verified, branded profile within the Truecaller	- Business phone numbers - Business profile information (name, logo, address, industry)	- Businesses using the verification service - Truecaller users

		application. This ensures that when the business calls a user, their official brand name, logo, and verification badge are displayed, distinguishing them from spam.	- Call logs and metadata (processed by Truecaller)	receiving calls from these businesses
7	FTEU Short Code	A "Free To End User" dedicated SMS short code (5-6 digits) where the business absorbs the cost of any reply messages from its customers. This encourages high-volume interaction for marketing campaigns, voting, or customer feedback.	- Phone number - Message content of the two-way conversation - Timestamps and delivery metadata	- Customers' end users - Mobile users participating in a campaign
8	Route Connector	An integration tool or API service that acts as a bridge, allowing a client's existing business systems (like CRM, ERP, or e-commerce platforms) to seamlessly connect to Route Mobile's communication APIs to trigger automated messages or calls.	- Any Personal Datapassed from the client's system, which can include: name, phone number, email address, customer ID, order details, or appointment information. The service acts as a data conduit.	- Customers' end users, employees, or other individuals whose data is stored in the client's integrated software.
9	Omnichannel - OCEAN	An integrated communication platform that unifies customer interactions across various channels like SMS, email, RCS and WhatsApp for a seamless experience. The integrated platform is called OCEAN	- All data categories from the individual channels it integrates (e.g., email address, phone number) - Customer interaction history across all channels - User behaviour – click rate, response rate, device details	- Customers' end users - Marketing leads - Employees
10	OmniCent	Omnicent is a payment gateway integration platform for the CPaaS channel to integrate with different payment instruments for different geographies	- All data categories from the individual channels it integrates (e.g., email address, phone number) - Customer payment history across channels	- Customers' end users - Marketing leads
11	Roubot	A tool for building custom chatbots with a codeless flow-builder and NLP engine integrations, deployable across web, social, and mobile channels. Roubot also allows live agents to communicate with end users through video.	- User input and conversation history - Name and user ID - Any Personal Datathe user provides during the chat - Phone Number	- Website visitors - Customers' end users interacting over 2-way channels with chatbots or Live-Agents
12	A2P Messaging	Application-to-Person (A2P) messaging allows businesses to send SMS messages to their users, often for alerts, OTPs, notifications, and marketing.	- Phone number - Message content - Timestamps, Delivery status and metadata	- Customers' end users - Application users - Employees
13	2-Way Messaging	Enables interactive, two-way	- Phone number	- Customers' end users

		SMS conversations between businesses and customers, allowing for replies and conversational engagement.	- Full conversation history (SMS content) - Timestamps and metadata	- Application users - Employees
14	Route OTP	A service for sending One-Time Passwords (OTPs) via SMS for user authentication and verification purposes.	- Phone number - Timestamps and verification status	- Customers' end users - Application users - Employees

ANNEX II - Technical and organisational measures including technical and organisational measures to ensure the security of data

1. Introduction

This document summarises the technical and organisational measures taken by the Processor within the meaning of Art. 32 (1) GDPR.

2. Confidentiality (Art. 32 para. 1 lit. b GDPR)

2.1 Physical access control

The following implemented measures prevent unauthorised persons from gaining access to the data processing systems:

- Alarm system
- Chip card/transponder locking system
- Personnel check at the gatekeeper or reception
- Visitors must be accompanied by employees
- Working from home: unauthorised persons have no access to employees' homes

2.2 System access control

The following implemented measures prevent unauthorised persons from gaining access to the data processing systems:

- Authentication with user and password
- Authentication with biometric data
- Use of anti-virus software
- Use of firewalls
- Use of mobile device management
- Encryption of data carriers
- Encryption of smartphones
- Automatic desktop lock
- Encryption of notebooks / tablets
- Management of user authorisations
- Creating user profiles
- Central password rules
- Use of 2-factor authentication
- Company policy on the use of mobile devices

2.3 Data access control

The following implemented measures ensure that unauthorised persons have no access to Personal Data:

- Number of administrators is kept as small as possible
- Management of user rights by system administrators

2.4 Separation control

The following measures ensure that Personal Datacollected for different purposes is processed separately:

1. Physically separate storage on separate systems or data carriers
2. Separation of production and test system
3. Encryption of data records that are processed for the same purpose
4. Logical client separation (on the software side)
5. For pseudonymised data: Separate storage of the allocation file on a separate, secure IT system (encrypted if possible)
6. Creation of an authorisation concept
7. Definition of database rights
8. Providing the data records with purpose attributes/data fields
9. Internal instruction to anonymise/pseudonymise Personal Datain the event of disclosure or after expiry of the statutory deletion period, if possible
10. Container apps when using private devices for business purposes (BYOD)

3. Integrity (Art. 32 para. 1 lit. b GDPR)

3.1 Transfer control

It is ensured that Personal Datacannot be read, copied, changed or removed without authorisation during transmission or storage on data carriers and that it is possible to check which persons or authorities have received Personal Data. The following measures have been implemented to ensure this:

- Provision of data via encrypted connections such as SFTP or HTTPS

3.2 Input control

The following measures ensure that it is possible to check who has processed Personal Datain data processing systems and at what time:

- Logging the entry, modification and deletion of data
- Manual or automatic control of the logs

4. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

The following measures ensure that Personal Datais protected against accidental destruction or loss and is always available to the client:

- Fire and smoke detection systems
- Hosting (at least of the most important data) with a professional hoster

5. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

5.1 Data protection management

The following measures are intended to ensure that the organisation meets the basic requirements of data protection law:

1. Use of the heyData platform for data protection management
2. Appointment of the data protection officer heyData
3. Obligation of employees to maintain data confidentiality
4. Regular data protection training for employees
5. Maintaining an overview of processing activities (Art. 30 GDPR)

5.2 Incident response management

The following measures are intended to ensure that reporting processes are triggered in the event of data protection violations:

- Reporting process for data protection violations in accordance with Art. 4 No. 12 GDPR to the supervisory authorities (Art. 33 GDPR)
- Notification process for data breaches in accordance with Art. 4 (12) GDPR to the Data Subjects (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data breaches
- Use of anti-virus software
- Use of firewalls

5.3 Data protection-friendly default settings (Art. 25 para. 2 GDPR)

The following implemented measures take into account the requirements of the principles of "privacy by design" and "privacy by default":

1. Training of employees in "privacy by design" and "privacy by default"
2. No more Personal Datais collected than is necessary for the respective purpose.

5.4 Order control

The following measures ensure that Personal Datacan only be processed in accordance with the instructions:

- Written instructions to the contractor or instructions in text form (e.g. through an data processing agreement)
- Ensuring the destruction of data after completion of the order, e.g. by requesting corresponding confirmations
- Confirmation from contractors that they commit their own employees to data secrecy (typically in the data processing agreement)
- Careful selection of contractors (especially regarding data security)