

# Data Processing Agreement

*This Data Processing Addendum ("DPA") is subject to the terms and conditions of, the Agreement between the Spectrm Ltd or the Spectrm Publishing UG (haftungsbeschränkt) (**Spectrm**) and the customer entity (**Customer**) that is a party according to the Terms of Services in their current version.*

## 1. Definitions

- I. "**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.
- II. "**Agreement**" means Spectrm's Terms of Service and Service Order Form, including any annexes or other written or electronic agreement.
- III. "**Customer Data**" means any personal data that Spectrm processes on behalf of Customer via the Service, as more particularly described in this DPA.
- IV. "**Data Protection Laws**" means all data protection laws and regulations applicable to a party's processing of Customer Data under the Agreement, including, where applicable, EU Data Protection Law and Non-EU Data Protection Laws.
- V. "**EU Data Protection Law**" means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); and (iii) in respect of the United Kingdom ("UK") any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union)
- VI. "**Non-EU Data Protection Laws**" means the California Consumer Privacy Act ("CCPA"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); and the Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018
- VII. "**SCCs**" means the standard contractual clauses for processors as approved by the European Commission or Swiss Federal Data Protection Authority (as applicable).
- VIII. "**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Customer Data on systems managed or otherwise controlled by Spectrm
- IX. "**Sensitive Data**" means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card

number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords; or (f) other information that falls within the definition of "special categories of data" under applicable Data Protection Laws.

X. The terms "**Personal Data**", "**controller**", "**data subject**", "**processor**", "**sub-processor**" and "**processing**" shall have the meaning given to them under Data Protection Laws or if not defined thereunder, the GDPR, and "process", "**processes**" and "**processed**" shall be interpreted accordingly.

## 2. Object

In accordance with Applicable Data Protection Laws, the Parties acknowledge and agree the following in relation to the Personal Data to be Processed under the Agreement:

<b>Nature of Processing</b>	Technical operation and further development of the chatbot service and marketing services.
<b>Purpose of Processing</b>	The data will be used to run, improve and personalize the service and for marketing related services.
<b>Type of Personal Data for using Messaging Service Facebook Messenger</b>	<ul style="list-style-type: none"> <li>• Facebook ID (page scoped)</li> <li>• All communication data connected with messages send to the service</li> </ul>
<b>Type of Personal Data for using Messaging Service Google Conversational Display Ads (Adlingo)</b>	<ul style="list-style-type: none"> <li>• Adlingo Session ID</li> <li>• All communication data connected with messages send to the service</li> </ul>
<b>Type of Personal Data for using Messaging Service WhatsApp</b>	<ul style="list-style-type: none"> <li>• Phone number</li> <li>• WhatsApp ID</li> <li>• All communication data connected with messages send to the service</li> </ul>
<b>Categories of Data Subjects</b>	The customers and/or end users of the Data Spectrms products and/or services who interacts with the chatbot

### 3. Roles and Responsibilities

- I. **Parties' roles.** If EU Data Protection Law or the LGPD applies to either party's processing of Customer Data, the parties acknowledge and agree that with regard to the processing of Customer Data, Customer is the controller and Spectrm is a processor acting on behalf of Customer, as further described in Annex C (Details of Data Processing) of this DPA.
- II. **Purpose limitation.** Spectrm shall process Customer Data only in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing ("**Permitted Purposes**"). The parties agree that the Agreement sets out Customer's complete and final instructions to Spectrm in relation to the processing of Customer Data, and processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.
- III. **Prohibited data.** Customer will not provide (or cause to be provided) any Sensitive Data to Spectrm for processing under the Agreement, and Spectrm will have no liability whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this DPA will not apply to Sensitive Data.
- IV. **Customer compliance.** Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its processing of Customer Data and any processing instructions it issues to Spectrm; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for Spectrm to process Customer Data for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Customer Data. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Data Protection Laws) applicable to any messages or other content created, sent or managed through the Service, including those relating to obtaining consents (where required) to send messages and the content of the messages.
- V. **Lawfulness of Customer's instructions.** Customer will ensure that Spectrm's processing of the Customer Data in accordance with Customer's instructions will not cause Spectrm to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. Spectrm shall promptly notify Customer in writing, unless prohibited from doing so under EU Data Protection Laws, if it becomes aware or believes that any data processing instruction from Customer violates the GDPR or any UK implementation of the GDPR.
- VI. **Updates to Security Measures.** Customer is responsible for reviewing the information made available by Spectrm relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures (Annex A) are subject to technical

progress and development and that Spectrm may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service provided to Customer.

## 4. Spectrm Compliance

Spectrm shall, comply with the following requirements:

- I. **Technical and organizational measures.** Implement and maintain appropriate technical and organizational measures in such a manner that the Processing of Personal Data will meet the requirements under Applicable Data Protection Laws and ensure the protection of the rights of the Data Subjects, and to regularly test, assess and evaluate the effectiveness of and, as necessary, improve and update these measures. The measures shall ensure a level of data security appropriate to the risks for the rights and freedoms of the Data Subjects. In particular, Spectrm shall protect the Personal Data against accidental or unlawful destruction, loss or alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed. Spectrm's technical and organizational measures shall include and comply with, at a minimum, the measures and requirements set forth in Annex A. Spectrm may change the agreed technical and organizational measures, provided that (i) Spectrm shall not provide for measures that deliver a level of protection that is materially lower than that provided for in Annex A and, in any event, the level of protection as required under the Applicable Data Protection Laws will be maintained, and (ii) Customer will be notified of any relevant changes to the technical and organizational measures with at least one (1) week prior notice
- II. **Confidentiality.** Ensure the reliability of any person authorized, including employees, agents and contractors, who may have access to Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the Personal Data, as strictly necessary for the Services, ensuring that all such individuals are subject to documented confidentiality undertakings.
- III. **Incident policies and procedures.** Implement and maintain security incident management policies and procedures. Spectrm promptly (but in any event no later than twenty-four (24) hours) notifies customer of any 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 (Personal Data Breach) or any other violation of this Appendix or Applicable Data Protection Laws as well as any reasonable suspicion of the occurrence of a Personal Data Breach or any other violation of this Appendix or Applicable Data Protection Laws; Spectrm shall cooperate with customer to fully address the matter and comply with all Applicable Data Protection Laws. Spectrm shall provide all relevant information to Customer, including the following: (i) a description of the nature of the incident; (ii) the name and contact information of a point of contact where additional information may be

obtained; and (iii) a description of measures taken or proposed to be taken to remedy the incident, including measures to mitigate negative effects.

- IV. **Data subject requests.** If Spectrm receives a request from a Data Subject whose Personal Data has been provided under the Agreement, including a request to directly exercise the Data Subject's rights, Spectrm shall promptly inform Customer of such request without responding to that request allowing Customer to handle these requests unless it has been otherwise authorized to do so by Customer. Spectrm shall cooperate with Customer as is necessary to respond to such requests.
- V. **Assist on compliance.** Spectrm shall provide reasonable assistance to Customer to ensure compliance with Customers obligations under Applicable Data Protection Laws, in particular, by providing all information and assistance to enable Customer (i) to comply with applicable data security obligations, and (ii) to carry out data protection impact assessments, and prior consultations with the supervisory authorities, where Customer is required to do so by Applicable Data Protection Laws, and (iii) to respond promptly and properly to any enquiries concerning the Processing of Personal Data and cooperate in good faith with the supervisory authorities or any third party within a reasonable time. Spectrm shall promptly inform Customer of any requests of any supervisory authority or third party concerning the Processing of Personal Data.
- VI. **Data retention.** Spectrm keeps Personal Data no longer than necessary for the purposes for which it was processed. In no event shall Spectrm keep such Personal Data for longer than ninety (90) calendar days following completion of the legitimate business purposes for which it was processed, unless agreed to by Customer in writing ("**Retention Period**"). At the conclusion of the Retention Period, or upon expiration or earlier termination of the Agreement, Provider shall securely delete Personal Data in accordance with this Agreement. In such a case, Provider warrants that it will guarantee the confidentiality of Personal Data and will not actively process Personal Data anymore.

## 5. Sub-processing

- I. **Engagement of Sub-processors.** Customer agrees that Spectrm may engage Sub-processors to process Customer Data on Customer's behalf. Customer authorizes Provider to (i) engage those other Processors listed in Annex C and/or (ii) to engage Sub-Processors not listed in Annex C. Provider shall inform Customer of any engagement of Sub-Processors not listed in Annex C, in particular by providing name, address and activities of such other Processors, regardless of whether such Sub-Processors are engaged by Provider or any other Processor, thereby giving Customer the opportunity to object to the use of such Sub-Processors.
- II. **Objection to Sub-processors.** Customer may object in writing to Spectrm's appointment of a new Sub-processor within five (5) calendar days of receiving notice in accordance with Section 3.1 of DPA, provided that such objection is based on

reasonable grounds relating to data protection. In such an event, the parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Spectrm will, at its sole discretion, either not appoint such Sub-processor, or permit Customer to suspend or terminate the affected Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

III. **Same level protection.** With respect to any other Processor engaged by Spectrm, Spectrm shall (i) before such other Processor first Processes Personal Data carry out adequate due diligence to ensure that such other Processor is capable of providing the level of protection for Personal Data required by this agreement.

## 6. Final clauses

- I. **Termination.** This DPA shall remain in effect for as long as Spectrm carries out Customer Data processing operations on behalf of Customer or until termination of the Agreement.
- II. **Previous agreements.** The parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Service.
- III. **Order of Precedence.** In the event of any conflict or inconsistency between this DPA and the Spectrm Terms of Service, the provisions of the following documents (in order of precedence) shall prevail: (a) SCCs; then (b) this DPA; and then (c) the Spectrm Terms of Service.
- IV. **Usage of Service Data.** Notwithstanding anything to the contrary in the Agreement (including this DPA), Spectrm shall have a right to collect, use and disclose Service Data for its legitimate business purposes, such as: (i) for accounting, tax, billing, audit, and compliance purposes; (ii) to provide, develop, optimize and maintain the Service; (iii) to investigate fraud, spam, wrongful or unlawful use of the Service; and/or (iv) as required by applicable law.
- V. **Limitation of Liability.** Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of liability set forth in the Agreement. Any claims made against Spectrm under or in connection with this DPA (including, where applicable, the SCCs) shall be brought solely by the Customer entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

## Annex A – Security Measures

In accordance with the obligations under this agreement the provider complies with his own information security policies. The applicable security policies can be found [here](#).

## Annex B – Jurisdiction-Specific Terms

California:

- I. The definitions of: “controller” includes “Business”; “processor” includes “Service Provider”; “data subject” includes “Consumer”; “personal data” includes “Personal Information”; in each case as defined under CCPA.
- II. For this “California” section of Annex B only, “Spectrm Services” means the suite of conversational marketing tools and insights available for Spectrm Customers to use, as may be further described in the Service Order Form and/or on the Spectrm Site.
- III. For this “California” section of Annex B only, “Permitted Purposes” shall include processing Customer Data only for the purposes described in this DPA and in accordance with Customer’s documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, as otherwise agreed in writing, or as otherwise may be permitted for “service providers” under the CCPA.
- IV. Spectrm’s obligations regarding data subject requests, as described in Section 4, IV (Data Subject Rights and Cooperation) of this DPA, apply to Consumers rights under the CCPA.
- V. Notwithstanding any use restriction contained elsewhere in this DPA, Spectrm shall process Customer Data only to perform the Spectrm Services, for the Permitted Purposes and/or in accordance with Customer’s documented lawful instructions, except where otherwise required by applicable law.
- VI. Spectrm may de-identify or aggregate Customer Data as part of performing the Service specified in this DPA and the Agreement.
- VII. Where Sub-processors process the personal data of Customer contacts, Spectrm takes steps to ensure that such Sub-processors are Service Providers under the CCPA with whom Spectrm has entered into a written contract that includes terms substantially similar to this DPA or are otherwise exempt from the CCPA’s definition of “sale”. Spectrm conducts appropriate due diligence on its Sub-processors.

Canada:

- I. Spectrm takes steps to ensure that Spectrm's Sub-processors, as described in Section 3 (Sub-processing) of the DPA, are third parties under PIPEDA, with whom Spectrm has entered into a written contract that includes terms substantially similar to this DPA. Spectrm conducts appropriate due diligence on its Sub-processors.
- II. Spectrm will implement technical and organizational measures as set forth in Section 4 (Spectrm Compliance) of the DPA.

### Annex C – Sub processors

<b>Name of Processor</b>	<b>Service provided</b>	<b>Address</b>	<b>Country</b>
Amazon Web Services Inc.	Third-party hosting provider.	410 Terry Avenue North Seattle WA 98109	United States
Amazon Web Services Germany GmbH.	Third-party hosting provider.	Krausenstr. 38, 10117 Berlin, Germany	Germany
Data Dog Inc.	Application performance monitoring, infrastructure and network monitoring, and error capturing. Spectrm may provide End User or dashboard Customer metadata, such as user identifiers, to DataDog for support and application troubleshooting and to improve performance of the Spectrm Services.	620 8th Avenue, Floor 45, New York, NY 10018	United States
Sentry, registered under Functional Software, Inc	Error tracking platform used by the Spectrm Services to capture errors that occur in the Spectrm Services. Spectrm may include dashboard	5 Fremont Street, 8th Floor, San Francisco, CA 94105.	United States



	Customer metadata such as user identifiers to Sentry for support and application troubleshooting and improving performance.		
Google LLC (Google Cloud Platform)	BigQuery is used as business intelligence software used to analyze Customer Data to identify trends and business outcomes	1600 Amphitheatre Pkwy Mountain View, CA 94043 United States	

## Signatures

The parties' authorized signatories have duly executed this DPA

**Spectrm Ltd**

Signature: \_\_\_\_\_

Printed: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**Customer:** \_\_\_\_\_

Signature: \_\_\_\_\_

Printed: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_