DATA PROCESSING AGREEMENT

This Data Processing Addendum ("DPA") is entered into between Webklipper Technologies Private Limited (including its Subsidiaries), hereinafter referred to as "WebEngage/Processor" and Customer and its Affiliates to enable WebEngage to process the Customer Personal Data as per the Applicable Data Privacy Laws while providing Services to the Customer("Services"). The DPA shall form an integral part of the Master Services Agreement and shall come into effect on the same date as the execution of the Order Form. In the course of providing the Services to Customer pursuant to the Agreement, WebEngage may Process Personal Data on Customer's behalf, and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

WHEREAS:

A. The Customer acts as a Data Controller (as defined below) in accordance with the Data Protection Laws (as defined below).

B. The Customer wishes to subcontract certain Services (defined below) that involve the Processing (defined below) of Personal Data (defined below), including Customer Personal Data (defined below), to the Processor.

C. The purpose of this DPA is to enable the Processor to Process on behalf of the Customer, Personal Data including Customer Personal Data necessary to perform the Services, define the conditions under which the Processor will Process Personal Data including Customer Personal Data to which it has access for the purpose of providing Services, and establish the obligations and responsibilities of the Processor while Processing Personal Data including Customer Personal Data for the purpose of providing Services **("Purpose")**. In the event of conflict, the Order Form shall prevail over this DPA solely with respect to the processing scope.

D. The Parties seek to implement a DPA that complies with the requirements of the current legal framework governing Data Protection Laws.

E. The Parties wish to lay down their rights and obligations in this DPA.

F. This DPA applies solely to Personal Data processed by the Processor on behalf of the Customer in connection with the Services.

G. Personal Data processed by WebEngage in its capacity as an independent Data Controller, including business contact data, marketing, sales, recruitment, security, compliance, and corporate administration data, is expressly excluded from the scope of this DPA and is governed by WebEngage's Privacy Policy.

1. Definitions

a) "**Affiliates**" means any entity that directly or indirectly controls, is controlled by, or is under common Control with the subject entity;

b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws and regulations of the India, European Union, the EEA and/or their member states, Switzerland and/or the United Kingdom, and of any other places where the customer is located (b) is permitted to use the Services pursuant to this DPA;

c) "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Customer;

d) "**Contracted Sub-Processor"** means any person appointed by or on behalf of the Processor to process Personal Data on behalf of the Customer in connection with this DPA;

e) "**Data Controller**" means the entity which determines the purposes and means of the Processing Personal Data;

f) **"Data Protection Laws**" means all applicable laws, regulations, rules, guidelines, or other legal requirements relating to data protection, privacy, confidentiality, security, or the Processing of Personal Data, in force in any jurisdiction where the Services are provided, where Personal Data is processed, or where Data Subjects are located. This includes, without limitation and as updated as of December 2025: in India, the Digital Personal Data Protection Act, 2023 (DPDP Act) together with the draft Digital Personal Data Protection Rules, 2025 (currently under public consultation); in the European Union/EEA/UK, Regulation (EU) 2016/679 (GDPR), UK GDPR, and implementing laws; in the United States, applicable federal and state laws (e.g., CCPA/CPRA as amended, HIPAA where relevant); in Saudi Arabia (KSA), the Personal Data Protection Law (PDPL, Royal Decree No. M/19 as amended by Royal Decree No. M/148), its Implementing Regulations, Regulations on Personal Data Transfers outside the Kingdom, and guidelines issued by the Saudi Data & Artificial Intelligence Authority (SDAIA); in Egypt, the Personal Data Protection Law No. 151/2020 (PDPL) and its executive regulations; in the United Arab Emirates (UAE), Federal Decree-Law No. 45/2021 on the Protection of Personal Data (PDPL, with executive regulations pending), and in financial free zones such as the Dubai International Financial Centre (DIFC Data Protection Law No. 5/2020 as amended) or Abu Dhabi Global Market (ADGM) regulations; and in other jurisdictions, equivalent frameworks such as LGPD (Brazil), PIPL (China), or PDPA (Singapore).

g) "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates;

h) "**Data Transfer**" means:
Transfer of Personal Data, including Customer Personal Data, from the Customer to a Contracted Processor; or an onward transfer of Personal Data, including Customer Personal Data, from a Contracted Processor to a Contracted Sub-Processor, or between two establishments of a Contracted Processor, in each case, where the applicable Data Protection Laws would regulate such transfer. Where required, transfers shall be conducted under lawful transfer mechanisms recognised under applicable law.

i) "**EEA**" means the European Economic Area;

j) "**EU**" means European Union;

k) "**EU Data Protection Laws"** means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

l) **"GDPR"** means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and

on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

m) "**Personal Data**" means any information relating to (i) an identified or identifiable natural person ("**Data Subject**") who can be identified, directly or indirectly, in particular by reference to an identifier such as name, location data, telephone numbers, identification number, e-mail addresses and other unique identifiers of such Data Subject, whether online or offline, or any combination of such identifier with any other information, and shall include any inference drawn from such data for profiling and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws);

n) "**Personal Data Breach**" means any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, Personal Data that compromises the confidentiality, integrity or availability of Personal Data of a Data Subject;

o) "**Processing**"/**"Process"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

p) "**Services**" shall mean and include Processor providing the Customer with an explicitly limited right to access and use the Dashboard and/or E-Mail services and/or SMS services and/or WhatsApp services, as subscribed to by the Customer.;

q) "**Supervisory Authority**" means an independent public authority established by an EU Member State pursuant to the GDPR, and independent public authorities established by other countries in accordance with their own data protection laws and regulations.

r) **"Technical and Organizational Measures"** means security measures, consistent with the type of Personal Data including Customer Personal Data being Processed and the services being provided by the Processor, to protect Personal Data including Customer Personal Data, which measures shall implement industry accepted protections which may include physical, electronic and procedural safeguards to protect the Personal Data including Customer Personal Data supplied to the Processor against any Personal Data Breach, and any security requirements, obligations, specifications or event reporting procedures outlined in this DPA or in. As part of such security measures, Processor shall provide a reasonably secure environment for all Personal Data, including Customer Personal Data, and for any hardware and software (including servers, networks, and data components) provided or used by the Processor in the performance of the Services.

1.1 **Interpretation**

(a) References to the singular shall include references to the plural and vice versa, as the context may require.

(b) References to one gender shall include references to the other gender, as the context may require.

(c) Any reference to 'Clause', 'Recital' or 'Schedule' shall be a reference to a clause, recital or schedule of this DPA.

(d) Headings and sub-headings are inserted only for ease of reference and shall not affect the construction or interpretation of this DPA.

(e) References to 'Controller' and 'Processor' shall be read as 'Data Fiduciary' and 'Data Processor' respectively, where the DPDP Act applies.

2. Term

This DPA shall be valid for 01 (one) year from the Effective Date ("Term"), which will be extended on an auto-renewal basis for one-year periods on each anniversary of the Effective Date, until the Customer continues to share Personal Data, including Customer Personal Data, with the Processor.

3. Processing of Customer Personal Data

3.1. In Processing Personal Data, including Customer Personal Data, on behalf of the Customer in connection with the provision of the Services, Processor shall:

(a) Comply with all applicable Data Protection Laws in the Processing of Personal Data, including Customer Personal Data;

(b) Immediately inform the Customer if the Processor thinks that an instruction of the Customer regarding the Processing of Customer Personal Data, including Personal Data, infringes the applicable Data Protection Laws.

(c) Process Personal Data including Customer Personal Data solely for the purpose of providing the Services and in accordance with the terms of this DPA or any other Customer's documented instructions and not for any other purpose, unless required to do so by applicable Data Protection Laws to which the Processor is subject, in which case Processor shall promptly inform Customer in writing of that legal requirement before commencing Processing unless that law prohibits such information on substantial grounds of public interest;

(d) Adopt and maintain the Technological and Organisational Security Measures outlined in Annexure-B;

(e) Ensure that all Personnel of Processor, including its agents, representatives, employees and subcontractors that Process Personal Data, including Customer Personal Data, for providing Services are subject to binding confidentiality and data protection obligations, and provide at minimum the same level of data protection that is required of the Processor under this DPA;

(f) Provide full co-operation and assistance to the Customer as reasonably necessary for the Customer to comply with its obligations under applicable Data Protection Law including but not limited to maintaining Personal Data secured, responding to Personal Data Breach, and, where applicable, ensuring obligations in respect of the rights of Data Subjects, carrying out Personal Data impact assessments, as may be appropriate or required under the relevant Data Protection Laws and assisting in consulting with competent authorities under the applicable Data Protection Laws.

(g) Notify the Customer without undue delay (and no later than 72 hours) of any request to the Processor by a Data Subject to exercise rights under Data Protection Law, such as to access, rectify, amend, correct, share, delete or cease Processing his/her Personal Data. Processor shall ensure that it does not respond to such a request except on the documented instructions of Customer or as required by applicable Data Protection Laws to which the Processor is subject, in which case Processor shall, to the extent permitted by such applicable Data Protection Laws, inform Customer of that legal requirement before the Processor responds to the request;

(h) With regards to the Processing of Personal Data, including Customer Personal Data, maintain a record of all Personal Data Processing activities carried out on behalf of the Customer;

(i) Not disclose Personal Data, including Customer Personal Data, to any third party (including, without limitation, Processor's subsidiaries and Affiliates and any person or entity acting on behalf of Processor) unless with respect to each such disclosure:

(A) The disclosure is necessary to carry out the Processor's obligations under this DPA;
(B) Processor executes a written agreement with such third party whereby such third party expressly assumes the same obligations outlined in this DPA;
(C) Processor has received the Customer's prior written consent to disclose;
(D) The processing is carried out in accordance with the instructions of the Customer; and
(E) Processor shall remain responsible for any breach of the obligations outlined in this DPA to the same extent as if Processor caused such breach.

(j) Establish policies and procedures to provide all reasonable and prompt assistance to Customer in responding to all requests, complaints, or other communications received from any individual who is or may be the subject of any Personal Data Processed by Processor to the extent such request, complaint, or other communication relates to Processor's Processing of such Personal Data.

(k) Processor shall implement appropriate safeguards for cross-border transfers, including Standard Contractual Clauses or equivalent mechanisms, where required under applicable Data Protection Laws. Customer remains responsible for determining the legality of its use of the Services.

(l) Provide the Customer with a copy of all Personal Data, including Customer Personal Data, held by the Processor in the format and on the media reasonably requested by the Customer;

(m) Notify the Customer without undue delay (and in any event within 72 hours) when the Processor receives any complaint, notice or communication from any governmental authority, data protection authority or any other third party in relation to the Personal Data including Customer Personal Data that Processor Processes for the purpose of providing the Services or to either Party's compliance with applicable Data Protection Laws or with the terms of this DPA;

4. Processor Personnel

4.1 Processor shall take reasonable steps to ensure the reliability of any of its employees, representatives, agents or Contracted Sub-Processors (collectively "Personnel") who may have access to the Personal Data, including Customer Personal Data.

4.2 Processor shall ensure that in case any of its Personnel have access to Personal Data, including Customer Personal Data, then such access is strictly limited to those Personnel on a "need to know" basis who need to know or have access to the relevant Personal Data, including Customer Personal Data, strictly for performance of Services and in compliance with this DPA. Processor shall ensure that

its Personnel who have access to the Personal Data, including Customer Personal Data, comply with legal requirements under the applicable Data Protection Laws and the terms of this DPA. Processor shall ensure that all its Personnel who Process Personal Data, including Customer Personal Data, are subject to binding confidentiality and data protection obligations and provide at minimum the same level of data protection that is required of the Processor under this DPA. The Processor shall be fully responsible for all acts or omissions of its Personnel in the same manner as for its own acts or omissions.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing Personal Data including Customer Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Personal Data including Customer Personal Data implement appropriate managerial, technical, operational, organizational and physical security control means to ensure a level of security appropriate to the risk presented by Processing, including, but not limited to, as applicable:

a. the pseudonymization and encryption of Personal Data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
c. the ability to restore the availability and access to Personal Data promptly in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.
e. In assessing the appropriate level of security, the Processor shall take into account, in particular, the risks presented by Processing, including the risk of a Personal Data Breach.
f. WebEngage maintains an information security program aligned with ISO 27001 / SOC 2 standards.

6. Sub-Processing

a) The Customer hereby provides general authorisation for the Processor to engage Sub-processors to process Personal Data for the purpose of providing the Services.
b) The Processor shall maintain an up-to-date list of Sub-processors (as noted in Annexure A) and subject to revision from time to time.
c) The Processor shall ensure that all Sub-processors are subject to written agreements imposing data protection obligations no less protective than those set out in this DPA.

7. Personal Data Breach

Processor shall notify the Customer of any Personal Data Breach without undue delay (and in any event within 72 hours) of discovering a Personal Data Breach, in which case Processor shall:
(a) as part of such notification, describe the complete details about and the nature of the incident and, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data including Customer Personal Data records concerned, and explain the impact of such Personal Data Breach upon Customer and the Data Subjects whose Personal Data is affected by such Personal Data Breach;
(b) In no case, delay notification because of insufficient information, but instead provide and supplement notifications as information becomes available; and

(c) In cooperation with the Customer or another auditor mandated by the Customer, use its best efforts to investigate such Personal Data Breach and take all necessary and appropriate corrective action to remedy such breach and prevent a recurrence of such breach;

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Customer reasonably considers to be required Data Protection Law, as applicable, in each case solely in relation to Processing of Personal Data including Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Sub-Processors.

9. Deletion or return of Personal Data

Subject to applicable Data Protection Laws and the Customer's documented instructions, the Processor shall retain Personal Data, including Customer Personal Data, for one (1) year from the date of storage, on a rolling basis, and shall automatically and securely delete or irreversibly anonymise such data upon expiry, unless retention is required by law or expressly instructed by the Customer. Personal Data may also be retained as long as necessary to provide the Services. Upon termination or expiration of the agreement, the Processor shall immediately cease all Processing and, within thirty (30) days, at the Customer's choice, return all Personal Data or securely destroy it, including any copies in backups, and shall confirm in writing upon completion. Where retention of any Personal Data is legally required ("Retained Personal Data"), the Processor shall inform the Customer, limit Processing to what is legally required, maintain the confidentiality of such data, and continue to comply with the DPA with respect to such data.

10. Inspection rights

10.1 Processor shall make available information reasonably necessary to demonstrate compliance with this DPA.

10.2 Audits shall:
(a) be conducted no more than once in any twelve (12) month period;
(b) be subject to at least thirty (30) days' prior written notice;
(c) occur during regular business hours;
(d) be conducted at the Customer's expense; and
(e) not permit access to source code, trade secrets, or sensitive security architecture.

10.3 Processor may satisfy audit requests by providing third-party audit reports or certifications such as ISO 27001 or SOC 2, where applicable.

10.4 Information and inspection rights of the Customer arise only under Clause 10.2, to the extent that the DPA does not otherwise grant the Customer information and audit rights that meet the relevant requirements of Data Protection Law.

11. Confidentiality

Each Party must keep the terms of this DPA and information it receives about the other Party and its business in connection with this DPA ("**Confidential Information**") confidential and must not use or

disclose that Confidential Information without the prior written consent of the other Party, except to the extent that:
(a) disclosure is required by law;
(b) The relevant information is already in the public domain.

12. Authorized Affiliates

12.1 Contractual Relationship.

The Parties acknowledge and agree that, by executing the DPA, Processor enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorised Affiliates, thereby establishing a separate data processing agreement between the Customer and each such Authorised Affiliate subject to the provisions of this Clause 11 and Clause 12 (below). Each Authorised Affiliate agrees to be bound by the obligations under this DPA.

12.2 Communication.

The Processor shall be responsible for coordinating all communication with the Customer under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorised Affiliates.

12.3 Rights of Authorised Affiliates.

Where an Authorised Affiliate becomes a party to this DPA, it shall, to the extent required under the applicable Data Protection Laws, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

(a) Except where the applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against the Customer directly by itself, the parties agree that (ii) solely the Processor shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Processor shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Clause 13.2 below).
(b) The Processor, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, including Customer Personal Data, takes all reasonable measures to limit any impact on the Customer and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorised Affiliates in one single audit.

13. Indemnification

13.1 Notwithstanding anything to the contrary contained in this DPA, Processor shall defend, indemnify and hold harmless Customer in accordance with section 13.2 and its Affiliates and their authorized representatives, officers, directors, employees, agents from and against all losses, damages, claims (including third-party claims), liabilities, deficiencies, actions (including any proceeding brought before any court, regulatory body, arbitration panel or other tribunal), judgments, interest, awards, penalties, fines, cost or other expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder (collectively "**Claims**"), arising out of or resulting from the Processor's (including its Personnel) failure to comply with any of its obligations under this DPA. Processor's obligation to fully indemnify, defend, and hold harmless under this Clause shall survive termination or expiration of this DPA.

13.2 Notwithstanding anything to the contrary in this DPA, the Processor's total aggregate liability arising out of or in connection with this DPA shall not exceed the total fees paid or payable by the Customer to the Processor in the twelve (12) months preceding the event giving rise to the claim, except where such liability arises from fraud or willful misconduct.

13.3 The Processor acknowledges that any act of willful or negligent breach of its obligations under this DPA by the Processor (including breach by its Personnel) would cause the Customer irreparable harm, including reputational damage, for which the Customer may have no adequate remedies at law. Accordingly, the Processor agrees that the Customer and/or its Affiliate(s) will have the right to simultaneously and in addition to its other rights and remedies, to seek injunctive relief as a remedy or to prevent or curtail any actual or threatened breach by the Processor of its obligations hereunder or for any violation of this DPA, without first being obliged to resort to arbitration.

14. Governing Law and Jurisdiction

14.1 This DPA shall be governed by and construed in accordance with the laws of India, and, subject to Clause 13.2 (below), the courts at Mumbai, India, shall have the exclusive jurisdiction over any matter relating to, in connection with, or arising out of, this DPA.

14.2 In the event of any dispute, controversy or claim arising out of or relating to the transactions contemplated by this DPA, or the validity, interpretation, breach or termination of any provision of this DPA, or, claims seeking redress or asserting rights under any law (each a "**Dispute**"), the Customer and the Processor agree that the Parties shall negotiate in good faith in an attempt to resolve such Dispute(s) amicably. .Suppose such Dispute has not been resolved to the mutual satisfaction of the Customer and the Processor within thirty (30) business days after the initial notice of the Dispute (or such more extended period as the Parties may agree), In that case, the Dispute shall be referred to a binding arbitration under the Arbitration and Conciliation Act, 1996 (as amended from time to time). The seat and venue of arbitration shall be Mumbai, India. The arbitration proceedings shall be governed by the Arbitration and Conciliation Act, 1996, and shall be conducted in English. The arbitral tribunal shall also decide on the costs of the arbitration proceedings. The arbitral tribunal's award shall be substantiated in writing, and the Parties shall submit to the arbitral tribunal's award, which shall be enforceable in any competent court of law.

15. Assignment

This DPA and the rights, interests, benefits, duties and obligations hereunder shall not be novated, assigned or transferred, in whole or in part, by either Party except with the prior written consent of the other Party. Any act in derogation of the foregoing shall be null and void. However, for the Customer, such prior permission from the Processor shall not be required in the case of an assignment in connection with any merger, consolidation, reorganisation, restructuring, or sale of all or substantially all of its assets, or any similar transaction. Following any assignment permitted hereunder, the assignee shall have the same rights and obligations as the assignor and shall agree in writing to be bound by the terms and conditions of this DPA, and the assigning party shall notify the other party of such assignment within a reasonable period of time following the change in Control.

16. Notice

16.1 Any notice, communication or statement required to be given under this DPA shall be in writing. It shall be sent by hand delivery, registered post with postage prepaid and with acknowledgement due, receipted courier, or by electronic mail to the applicable Party at the contact details indicated below, or to such other address as a Party shall designate by similarly giving notice to the other Party.

Notice to be given to the Processor:
Address: B-1602, Lotus Corporate Park, off Western Express Highway, Goregaon (East), Mumbai, Maharashtra – 400063
Email: legal@webengage.com

16.2 Notice given under Clause 16.1 above shall be deemed to have been received:
(a) if delivered personally, on the day of delivery;
(b) if sent by courier, on the day of delivery;
(c) 5 (five) business days after posting if transmitted by registered post (including airmail);
(d) If sent by fax or electronic mail, on the day of transmission, subject to confirmation of uninterrupted transmission, whichever shall first occur.

17. Severability

Suppose any provision of this DPA or the application thereof to any person or circumstance shall be invalid or unenforceable to any extent for any reason, including by reason of any applicable laws. In that case, the remainder of this DPA and the application of such provision to persons or circumstances other than those as to which it is held invalid or unenforceable shall not be affected thereby. Each provision of this DPA shall be valid and enforceable to the fullest extent permitted by applicable laws. Suppose any provision or a part thereof of this DPA becomes or is declared by a court of competent jurisdiction to be illegal, unenforceable or void. In that case, the remaining provisions shall continue in full force and effect. The DPA shall be deemed to be reformed by replacing such invalidated or unenforceable provision with a valid and enforceable provision that gives effect as closely as possible to the intentions of the parties as expressed by the invalidated or unenforceable provision.

18. Entire Agreement and Alteration

18.1 This DPA constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes any prior negotiations, representations or agreements, either written or oral.

18.2 No modification, amendment, supplement or waiver of any provision of this DPA shall be effective unless made by a written instrument duly executed by both the Parties, which refers explicitly to this DPA. Both Parties agree that email shall be deemed a written instrument for this Clause.

19. Acceptance

Acceptance of this DPA by the Customer may be effected by electronic means, including by execution of an Order Form referencing the MSA, or by continued use of the Services after this DPA is made available. This DPA is accepted electronically by an authorised representative of the Processor through an electronic signing

For the Processor:

Webklipper Technologies Private Limited (WebEngage/Processor)

Avlesh Singh

Authenticated through Leegality.com
(01KCNBA85HCP3A6P7TRADNQ4QC)
Avlesh Singh
Date: Wed Dec 17 10:50:47 IST 2025

By: _____

Name: Avlesh Singh

Title: Director

Date:17th December,2025

Annexure A
List of Approved sub- processors

This Annexure forms part of the Data Protection Agreement (DPA) between the Data Controller and the Data Processor. It lists the authorised sub-processors engaged by the Data Processor to process personal data under the Agreement.
The Customer acknowledges and agrees that WebEngage may engage Sub-processors on an as-and-when-required basis to provide the Services availed by the Customer. WebEngage shall maintain a list of its current Sub-processors, which may be updated or modified from time to time at WebEngage's sole discretion. Any such updates shall apply automatically to the Services without requiring additional consent from the Customer, provided that WebEngage continues to comply with its obligations under this Agreement and applicable data protection laws.

Third-Party Vendors

Subprocessor Name	Registered Address	Processing Activities	Location of Processing	Data Categories Processed
Infobip	10th Floor, E Wing, Times Square, Andheri Kurla Road, Marol, Andheri East, Mumbai - 400059	SMS	Mumbai, India	PII & Non-PII
Infobip	10th Floor, E Wing, Times Square, Andheri Kurla Road, Marol, Andheri East, Mumbai - 400059	SMS	Frankfurt, Germany	PII & Non-PII
Infobip	10th Floor, E Wing, Times Square, Andheri Kurla Road, Marol, Andheri East, Mumbai - 400059	Conversations (Live Agent)	Frankfurt, Germany	PII & Non-PII
Infobip	10th Floor, E Wing, Times Square, Andheri Kurla Road, Marol, Andheri East, Mumbai - 400059	RCS	Mumbai, India	PII & Non-PII

Infobip	10th Floor, E Wing, Times Square, Andheri Kurla Road, Marol, Andheri East, Mumbai - 400059	Email	Mumbai, India	PII & Non-PII
Infobip	10th Floor, E Wing, Times Square, Andheri Kurla Road, Marol, Andheri East, Mumbai - 400059	Voice API	Mumbai, India	PII & Non-PII
Infobip	10th Floor, E Wing, Times Square, Andheri Kurla Road, Marol, Andheri East, Mumbai - 400059	WhatsApp	Mumbai, India	PII & Non-PII
Karix	Tanla Technology Centre, Hi Tech City Road, Madhapur, Hyderabad - 500081	WhatsApp	Chennai, India	PII & Non-PII
Karix	Tanla Technology Centre, Hi Tech City Road, Madhapur, Hyderabad - 500081	SMS	Chennai, India	PII & Non-PII
Karix	Tanla Technology Centre, Hi Tech City Road, Madhapur, Hyderabad - 500081	RCS	Chennai, India	PII & Non-PII
Karix	Tanla Technology Centre, Hi Tech City Road, Madhapur,	WhatsApp	Chennai, India	PII & Non-PII

	Hyderabad - 500081			
TANLA DIGITAL	Building 20, 1st Floor, Premises No 102 Dubai Internet City, Dubai, United Arab Emirates	SMS	United Arab Emirates	PII & Non-PII
Cequens	Business Center, Dubai World Central, P.O. Box 390667, Dubai, United Arab Emirates	SMS	Paris, France	PII & Non-PII
Cequens	Business Center, Dubai World Central, P.O. Box 390667, Dubai, United Arab Emirates	SMS	Saudi Arabia	PII & Non-PII
CM Telecom	16 Raffles Quay, #33-03 Hong Leong Building , 048581, Singapore	SMS	Amsterdam, Netherlands	PII & Non-PII
CM Telecom	16 Raffles Quay, #33-03 Hong Leong Building , 048581, Singapore	SMS	Eindhoven, Netherlands	PII & Non-PII
CM Telecom	16 Raffles Quay, #33-03 Hong Leong Building , 048581, Singapore	SMS	Singapore	PII & Non-PII
MailerCloud	1/213, B R Building, Iringalloor Ammathoor	Email	India	PII & Non-PII

	Padam, Guruvayurappan College PO, Kozhikode, Kerala, 673014			
Gupshup	1st Floor, Silver Metropolis, Western Express Highway, Goregaon (E), Mumbai 400063, India.	SMS	Mumbai, India	PII & Non-PII
Gupshup	1st Floor, Silver Metropolis, Western Express Highway, Goregaon (E), Mumbai 400063, India.	WhatsApp	Mumbai, India	PII & Non-PII
Gupshup	1st Floor, Silver Metropolis, Western Express Highway, Goregaon (E), Mumbai 400063, India.	RCS	Mumbai, India	PII & Non-PII
ValueFirst	Tanla Technology Centre, Hitech City Road, Madhapur, Hyderabad, Shaikpet, Telangana, India, 500081	SMS	India	PII & Non PII
ValueFirst	Tanla Technology Centre, Hitech City Road, Madhapur, Hyderabad, Shaikpet, Telangana, India, 500081	SMS	India	PII & Non PII

TelSpiel	17-18,Punj Essen House, Level-5, Nehru Place, New Delhi, South East Delhi, Delhi, 110019	RCS	Noida, India	PII & Non PII
TelSpiel	17-18,Punj Essen House, Level-5, Nehru Place, New Delhi, South East Delhi, Delhi, 110019	SMS	Noida, India	PII & Non PII
MSG91	405-406, Capt. C.S. Naidu Arcade, 10/2 Old Palasia, Indore, Madhya Pradesh	SMS	Mumbai, India	PII & Non PII
Caspar Technologies	7th Floor Chakolas Heights, Chittethukara, Kakkaknd-682037, Kerala	Email	Chicago, USA	PII & Non PII
Alot Digital	204, 2ND FLOOR RAGHULEELA MEGA MALL, POISAR GYMKHANA ROAD, KANDIVALI WEST MUMBA, MUMBAI-400067, MAHARASHTRA	SMS	Mumbai, India	PII & Non PII
V-Connect	1302, Saviour Greenisle, PLOT NO. GH-11, Crossing Republik, Ghaziabad, UP- 201016	SMS	Noida, India	PII & Non PII

V-Connect	1302, Saviour Greenisle, PLOT NO. GH-11, Crossing Republik, Ghaziabad, UP- 201016	RCS	Noida, India	PII & Non PII
Tata Communications	Tower 4, 4th to 8th Floor, Equinox Business Park, LBS Marg, Kurla (W) Mumbai 400070	SMS	Mumbai, India	PII & Non PII
Tata Communications	Tower 4, 4th to 8th Floor, Equinox Business Park, LBS Marg, Kurla (W) Mumbai 400070	RCS	Mumbai, India	PII & Non PII
Tata Communications	Tower 4, 4th to 8th Floor, Equinox Business Park, LBS Marg, Kurla (W) Mumbai 400070	Email	Mumbai, India	PII & Non PII
Tata Communications	Tower 4, 4th to 8th Floor, Equinox Business Park, LBS Marg, Kurla (W) Mumbai 400070	WhatsApp	Mumbai, India	PII & Non PII
OneXtel	C-802, 8th Floor ATS Bouquet, Sector 132, Noida, 201308	SMS	Germany	PII & Non PII
OneXtel	C-802, 8th Floor ATS Bouquet, Sector 132, Noida, 201308	SMS	Mumbai, India	PII & Non PII

OneXtel	C-802, 8th Floor ATS Bouquet, Sector 132, Noida, 201308	RCS	Mumbai, India	PII & Non PII
OneXtel	C-802, 8th Floor ATS Bouquet, Sector 132, Noida, 201308	SMS	Germany	PII & Non PII
TrustSignal	PLOT NO A-45-50, PIONEER HOUSE 4TH FLOOR, SECTOR-16, Gautam Buddha Nagar, NOIDA, Uttar Pradesh, India, 201301	RCS	- Mumbai, India - Bangalore, India	PII & Non PII
TrustSignal	PLOT NO A-45-50, PIONEER HOUSE 4TH FLOOR, SECTOR-16, Gautam Buddha Nagar, NOIDA, Uttar Pradesh, India, 201301	SMS	- Mumbai, India - Bangalore, India	PII & Non PII
RouteMobile	3rd Floor, 4th Dimension, Mind Space, New Link Road, Malad (W), Mumbai 400 064, India	SMS	Mumbai, India	PII & Non PII
RouteMobile	3rd Floor, 4th Dimension, Mind Space, New Link Road, Malad (W), Mumbai 400 064, India	RCS	Mumbai, India	PII & Non PII

RouteMobile	3rd Floor, 4th Dimension, Mind Space, New Link Road, Malad (W), Mumbai 400 064, India	WhatsApp	Mumbai, India	PII & Non PII
RouteMobile	Office Number 14, Building 7544, Othman Ibn Affan Road, At Taawun, Riyadh, Saudi Arabia	SMS International	Saudi Arabia	PII & Non PII
Bird	Keizersgracht 268, 1016 EV, Amsterdam, The Netherlands	Email	Netherlands	PII & Non PII
Bird	Keizersgracht 268, 1016 EV, Amsterdam, The Netherlands	Email	Belgium	PII & Non PII
Sinch	7th Floor, Tower - 4, Express Trade Tower - 2, Sector - 132, Noida - 201301, India	SMS	Mumbai, India	PII & Non PII
Sinch	7th Floor, Tower - 4, Express Trade Tower - 2, Sector - 132, Noida - 201301, India	RCS	Mumbai, India	PII & Non PII
Sinch	7th Floor, Tower - 4, Express Trade Tower - 2, Sector - 132, Noida - 201301, India	Email	Mumbai, India	PII & Non PII

Sinch	7th Floor, Tower - 4, Express Trade Tower - 2, Sector - 132, Noida - 201301, India	WhatsApp	Mumbai, India	PII & Non PII
Jio	Reliance Corporate Park TC 23, Central Rd N, Reliance Corporate Park, MIDC Industrial Area, Ghansoli, Navi Mumbai, Maharashtra 400701	RCS	Mumbai, India	PII & Non PII

Information and Analytics

Sub-processor Name	Category	WebEngage's Customer Information	Customers' Users Data	Region
Amazon Web Services, Inc. (Subsidiary of Amazon.com, Inc.)	Cloud Computing / Infrastructure as a Service (IaaS)	Yes	PII and non-PII	US, IN
Google LLC (Subsidiary of Alphabet Inc.)	Cloud Computing, Analytics, Advertising, Large Language Models	Yes	PII and non-PII	US, IN, KSA
Cloudflare, Inc.	Web Infrastructure & Security (CDN, WAF, DNS)	No	non-PII	US, IN
Datadog, Inc.	Monitoring & Analytics (Application Performance Monitoring)	No	non-PII	US
PagerDuty, Inc.	Incident Management Platform	No	non-PII	US
Zendesk, Inc.	Customer Support / Help Desk Software (SaaS)	Yes	PII and non-PII	US
OpenAI, L.L.C.	Artificial Intelligence - Large Language Model	No	non-PII	US
X Corp.	Artificial Intelligence - Large Language Model	No	non-PII	US
Salesforce, Inc.	Customer Relationship Management (CRM) Software (SaaS)	Yes	NA	US
LinkedIn Corporation (Subsidiary of Microsoft)	Advertising / Professional Networking	Yes	NA	US

Meta Platforms, Inc. (or one of its subsidiaries like Facebook Ireland Ltd.)	Advertising / social media	Yes	NA	US
G2.com, Inc.	Software Marketplace / Review Platform	Yes	NA	US
Google LLC (or a specific subsidiary)	Web Analytics	Yes	NA	US
HubSpot, Inc.	Marketing, Sales, & Service Software (SaaS)	Yes	NA	US
GTM Buddy Inc.	Sales Enablement / Revenue Enablement Software (SaaS)	Yes	NA	US
OneTrust	Consent (Cookie) Management Tool	Yes	NA	US
NextRoll, Inc	Advertising	Yes	NA	US

Subprocessor Approval & Compliance:

1. The Data Processor shall obtain prior written authorisation from the Data Controller before engaging any new Subprocessor.
2. All subprocessors must comply with applicable data protection regulations, including GDPR, CPRA, and DPDP.
3. The Data Processor shall ensure that each Subprocessor enters into a contract that imposes equivalent data protection obligations as outlined in the DPA.

Annexure B
Technical and Organisational Security Measures

This Annexure forms part of the Data Protection Agreement (DPA) between the Data Controller and the Data Processor. It outlines the technical and organisational measures implemented by the Data Processor to ensure the security, confidentiality, and integrity of personal data processed under this Agreement.

1. Data Protection Measures
- Encryption of personal data in transit and at rest using industry-standard encryption methods.
- Pseudonymization and anonymisation of personal data where applicable.
- Access control mechanisms to limit data access to authorised personnel only.
- Secure authentication processes, including multi-factor authentication (MFA).
- Data minimisation policies to ensure only necessary data is collected and retained.

2. Access Control and Identity Management
- Role-based access control (RBAC) to restrict data access based on job functions.
- Unique user identification and secure login credentials for all personnel.
- Regular review and revocation of access rights for employees and third parties.

- Monitoring and logging of access to sensitive personal data.
- Implementation of least privilege principles to restrict data access.

3. Network and System Security

- Implementation of firewalls, intrusion detection, and prevention systems.
- Regular vulnerability assessments and penetration testing.
- Security patch management to keep software and systems updated.
- Network segmentation to limit internal data access and exposure.
- Secure VPN and endpoint security solutions for remote access.

4. Incident Response and Breach Notification

- Defined incident response procedures for identifying, mitigating, and reporting security incidents.
- 24/7 monitoring and detection of security breaches.
- Breach notification processes to inform the Data Controller within 72 hours from the time of knowledge.
- Regular cybersecurity training and awareness programs for employees.
- Incident response drills and tabletop exercises are conducted periodically.

5. Business Continuity and Disaster Recovery

- Regular backup and recovery procedures for critical data.
- Offsite and encrypted backups to ensure data redundancy.
- Disaster recovery plans with defined recovery time objectives (RTOs) and recovery point objectives (RPOs).
- Regular testing of business continuity and disaster recovery plans.
- Alternate data processing locations to minimise disruptions.

6. Compliance and Audit

- Regular internal and external audits to ensure compliance with GDPR, CCPA, and DPDP.
- Documentation of all security policies, procedures, and risk assessments.
- Data protection impact assessments (DPIAs) for high-risk data processing activities.
- Compliance with industry standards such as ISO 27001, ISO 27701, and SOC 2.
- Periodic security training and awareness programs for employees.