DATA PROTECTION ADDENDUM

PARTIES

Wingify Contracting Entity ("**Wingify**" or "**Processor**")	**Wingify Software Private Limited**
Wingify Address	1104, KLJ Tower North, Netaji Subhash Place, Pitampura, Delhi, India
Customer Contracting Entity ("**Customer**" or "**Controller**")	**[Customer Name as mentioned in the Agreement]**
Customer Address	[Customer Address as mentioned in the Agreement]

ANNEXURES

This Data Protection Addendum ("**DPA**") includes the DPA Terms and Conditions below together with the following Annexures, which are appended hereto:

Annexure 1	Categories of User Data
Annexure 2	Technical and operational security measures

DPA TERMS AND CONDITIONS

1. INTERPRETATION

1.1. **Relationship with Agreement**. This DPA forms part of, and shall be co-terminus with the Agreement between the Customer and Wingify. This DPA shall be applicable to any Personal Data collected during the course of the Services provided under the Agreement. In the event of any conflict between the terms and conditions of the Agreement and the terms and conditions of this DPA, the latter shall prevail. Except as expressly provided otherwise herein, (i) all terms used in this DPA will have such meaning as provided under the Agreement, and (ii) all other terms and conditions of the Agreement shall apply to this DPA.

1.2. **Data Definitions**. For the purposes of this DPA:

(i) **"Personal Data"** means any information related to any identified or identifiable natural person.

(ii) **"User Data"** means Personal Data related to the Users (as defined under the Agreement), more specifically as detailed in Annexure 1 to this DPA.

(iii) "**Customer Account Data**" means any Personal Data other than User Data that is provided by the Customer or collected by Wingify from the Customer, during the Services and includes any Personal Data of any employee or other personnel of the Customer relating to the Customer's relationship with Wingify, including but not limited to, Personal data collected for Customer's account, billing or payment information of individuals that Customer has associated with its account, contact data required for managing its relationship with Customer, or as otherwise required by applicable laws and regulations.

1.3. **Other Definitions**. For the purposes of this DPA:

(i) "**Data Protection Laws**" means the relevant and applicable data protection and data privacy laws, rules, and regulations applicable to Personal Data.

(ii) "**Data Subjects**" shall mean any individual natural persons who can be identified directly or indirectly using any Personal Data.

(iii) "**Processing**" means any operation or set of operations performed on data or sets of data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. "Process," "Processes," and "Processed" shall have the same meaning.

(iv) "**Personal Data Breach**" means any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Personal Data.

(v) "**Services**" means the services provided to the Customer or any other activities performed on behalf of the Customer by Wingify, pursuant to the Agreement.

(vi) "**Sub-Processor**" means any third-party appointed by or on behalf of Wingify to Process Personal Data on behalf of the Customer in connection with the Agreement.

(vii) "**Standard Contractual Clauses**" means (i) where GDPR applies, the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021, available at https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32021D0914&qid=1623940939861 ("EU SCCs"); or (ii) where the UK GDPR applies, the standard data protection clauses for processors adopted pursuant to or permitted under Article 46 of the UK GDPR ("UK SCCs"); in each case as may be amended, superseded or replaced from time to time.

2. DATA PROCESSING

2.1. **User Data Collection**. The Services are offered in a manner that enables the Customer to determine the nature and extent of User Data that is collected and provided to Wingify for Processing in the manner described in Annexure 1. Wingify shall ensure that sufficient technical measures are provided to enable the Customer to make such determination. Wingify shall not Process any other User Data other than those specified in Annexure 1.

2.2. **Consents**. Customer shall ensure compliance with all Data Protection Laws while collecting and providing any Personal Data to Wingify, including without limitation, ensuring that all required consents, to the extent applicable, have been taken from Users and/or other data subjects.

2.3. **Customer Processing Instructions**. Wingify shall comply with, and Process all User Data according to, the written and documented instructions received from the Customer and in the manner described under this DPA (including Annexure 1). Wingify shall endeavour to inform the Customer if it reasonably believes that any of the instructions received from the Customer violate any of the Data Protection Laws. Such notification will not constitute a general obligation on part of Wingify to monitor and interpret the laws applicable to the Customer, and such notification will not constitute legal advice to the Customer.

2.4. **Use of User Data**. Unless otherwise instructed to by the Customer, the User Data shall be used only for the following purposes:

(i) Processing and storage necessary to provide the Services;

(ii) to provide product support to the Customer; and/or

(iii) disclosures as required by law or otherwise as set forth in the Agreement.

2.5. **Use of Customer Account Data**. Customer Account Data shall be used only used for the following purposes:

(i) to provide product support to the Customer; and/or

(ii) disclosures as required by law, necessary to enforce any rights of Wingify under the Agreement, or otherwise as set forth in the Agreement.

3. WINGIFY RESPONSIBILITIES

3.1. **Compliance with Data Protection Laws**. Wingify shall comply with all applicable Data Protection Laws in the Processing of any User Data.

3.2. **Technical & Organisational Security Measures**. Wingify shall maintain administrative, physical, and technical safeguards for protection of the security, confidentiality, integrity, and privacy of User Data. Such measures are set out in Annexure 2. Wingify monitors compliance with these safeguards. Customer acknowledges that such security & privacy measures are subject to technical progress and development and

that Wingify may update or modify the security & privacy measures at its sole discretion from time to time, provided that such updates and modification do not result in the degradation of the overall security & privacy of the Services used by the Customer.

3.3. **Personnel**. Wingify shall ensure that its personnel engaged in the Processing of User Data are informed of the confidential nature of the User Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality and such obligations survive the termination of that person's engagement with Wingify. Wingify shall take commercially reasonable steps to ensure the reliability of any Wingify personnel engaged in the Processing of User Data. Wingify shall ensure that access to User Data and Personal Data is limited to those personnel who require such access to perform the Services.

3.4. **Data Protection Officer**. Wingify has appointed an EU representative as mandated under GDPR and a Data Protection officer to monitor Wingify's data privacy compliance globally. The appointed person can be reached by email via privacy@wingify.com

4. SUB-PROCESSORS

4.1. **Authorized Sub-Processors**. Customer agrees that Wingify may engage Sub-Processors to Process User Data on Customer's behalf or provide the Services as provided in: https://vwo.com/compliance/subprocessors

4.2. **Obligations of Sub-Processors**. Wingify shall (i) enter into written agreement with the Sub-Processor imposing data protection terms that require the Sub-Processor to protect the User Data to the standard required by Data Protection Laws, and (ii) remain responsible for its compliance with the obligations of the DPA and for any acts or omissions of the Sub-processor that cause Wingify to breach any of its obligations under this DPA.

5. CROSS-BORDER DATA TRANSFERS

5.1. **Location**. All User Data is stored in the United States of America, unless the terms regarding storage of User Data in the European Union have been mutually agreed in writing between Customer and Wingify.

5.2. **European Commission Standard Contractual Clauses**. To the extent Wingify transfers or Processes any User Data relating to Data Subjects in the European Union outside the European Union, all actions in relation to such User Data shall be governed by the Standard Contractual Clauses as currently applicable under Regulation (EU) 2016/679 of the European Parliament and the Council of the European Union (GDPR).

For the purposes of such Standard Contractual Clauses:

(i) the Customer shall be the "Controller" and the "data exporter" and Wingify shall be the "Processor" and the "data importer";
(ii) the parties agree that Module Two (Controller to Processor) of the Standard Contractual Clauses shall be applicable;
(iii) all references to "Annex I.A" shall instead refer to the information in this section and in page 1 of the DPA;
(iv) all references to "Annex I.B", shall instead refer to Annexure 1 of this DPA; and
(v) all references to "Annex II.B", shall instead refer to Annexure 2 of this DPA.

6. CERTIFICATIONS AND AUDITS

6.1. **Certifications.** Wingify has obtained privacy and security assessments and certifications by third parties, details of which can be found at https://vwo.com/compliance/.

6.2. **Records**. Wingify agrees to keep records of its Processing in compliance with Data Protection Laws and provide such records to Customer upon reasonable request to assist Customer in complying with any regulatory request.

6.3. **Reports and Audit**. Wingify shall maintain records of its security standards. Upon Customer's request, Wingify shall provide (on confidential basis) copies of relevant external third-parties audit report

summaries, certification and/or other documentation reasonably required by Customer to verify Wingify's compliance with this DPA. Wingify shall further provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires, that Customer reasonably considers necessary to confirm Wingify's compliance with this DPA.

6.4. **Additional Independent Audit**. To extent the audit reports, certification, documentation and/or third-party audit reports mentioned above are not sufficient to demonstrate compliance with the obligation in this DPA, the Customer may execute or appoint a third-party independent auditor in such an event, the parties agree that.

(i) Customer is responsible for all costs and fees relating to such audit;

(ii) A third-party auditor (not being a competitor of Wingify) must be mutually agreed upon between the parties and such auditor shall follow industry standard and appropriate audit procedures;

(iii) The Controller's right to audit shall be subject to giving the Processor at least 4 weeks prior written notice of any such audit at privacy@wingify.com. The notice period for the right to audit may be reduced as per mutual discussion is such audit is required as part of an investigation by a regulator;

(iv) Such audit must not unreasonably interfere with Wingify's business activities and must be reasonable in time and scope of Services;

(v) The parties must agree to a specific audit scope and plan prior to any such audit, which must be negotiated in good faith between the parties; and

(vi) For any audit of any Sub-Processors, Wingify shall endeavour to provide all commercially reasonable assistance to facilitate such audit.

7. INCIDENT RESPONSES AND COMMUNICATIONS

7.1. **Notice of Non-Compliance**. If Wingify cannot provide compliance or foresees that it cannot comply with its obligations as set out in this DPA, it agrees to promptly inform the Customer of the same. Upon such notice, the Customer is entitled to suspend the transfer and processing of any User Data or Customer Account Data.

7.2. **Notice of Personal Data Breach**. Wingify will notify Customer promptly and without undue delay of an actual or potential Personal Data Breach or any security exposure of Customer system or data relating to the Personal Data Breach as it becomes known or as is reasonably requested by Customer. Wingify's notification of a Personal Data Breach will describe, to the extent possible, the nature of the Personal Data Breach, the measures taken to mitigate the potential risks and the measures that Wingify recommends Customer take to address the Personal Data Breach.

7.3. **Consequences of a Personal Data Breach Notification**. Wingify shall promptly take reasonable steps to minimize harm and secure User Data in the event of a Personal Data Breach. Wingify's notification of or response to a Personal Data Breach will not be construed as an acknowledgment by Wingify of any fault or liability with respect to the Personal Data Breach.

7.4. **Data Subject Requests**. Any request from a data subject directly to Wingify shall be directed to the Customer. Upon instruction by the Customer, Wingify shall correct, rectify, or block any User Data to the extent they can be done by Wingify. Wingify shall cooperate to the necessary extent and provide the Customer with appropriate support wherever possible in the fulfilment by the Customer of the rights of the Data Subjects under any applicable Data Protection Laws, in the preparation of records of processing activities, and in the case of necessary data protection impact assessments by the Customer. Except as specified above, Wingify has no obligation to assess any Personal Data in order to identify information subject to any specific legal requirements.

7.5. **Confidentiality**. Information that may be disclosed in any form between Parties with respect to, or as a result of this DPA, shall be deemed to be Confidential Information (as defined under the Agreement). Information relating to Wingify's database, procedures, and processes shall be considered Confidential Information.

8. DISPOSAL AND RETENTION OF USER DATA

8.1. **Disposal of User Data**. Wingify shall promptly and in any event between 45 to 90 days of the date of termination/expiry of the Agreement, or upon request, delete all User Data in accordance with Wingify's procedure.

8.2. **Retention of User Data**. Wingify may retain User Data to the extent required by applicable laws and only to the extent and for such period as required by applicable laws, provided that the provisions of this DPA will continue to apply in respect of any User Data retained during the duration of such retention.

9. LIABILITY

9.1. **Limitation of Liability**. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to the Agreement or this DPA, whether in contract, tort, or under any other theory of liability, is subject to the "Limitation of Liability," as mentioned in the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party under the entire Agreement, including this DPA.

[END OF DPA TERMS AND CONDITIONS]

ANNEXURE 1: CATEGORIES OF USER DATA

Categories of User Data	Information stored by VWO	Examples	Nature and Purpose of Processing	Is it possible to identify data subject with this data
Geo location (configurable by Customer)	Country, Region and City name only	San Francisco, California, US	Country-based information and used only for data segmentation. Customer can configure it to store just Country / Country & Region / Country, Region & City, or completely turn it off.	No
Internet Protocol (IP) address (configurable by Customer)	Anonymized IP address (last octet removed by default)	10.16.72.0 10.16.0.0 10.0.0.0 0.0.0.0	Wingify uses an IP de-identification mechanism that automatically masks a portion of each visitor's IP (Internet Protocol), effectively making it impossible to identify a particular individual solely via their IP address. Wingify adheres to privacy by design and default principle, IP address stored without the last octet by default, and this is configurable by Customer up to complete removal. This means, no individual or data subject can be tracked or identified by Wingify.	No
Cookies (Online Identifier)	UUID (Universally unique identifier)	4201E4DB-4C25-BA4DDD31-C137C7 18D30E	A randomly generated UUID (Universally unique identifier) with no finger printing information of the User is created and stored on the browser. A one-way hashed value is stored in Wingify databases or DBs (pseudonymization).	No
Additional Categories of Information to be Processed for 'VWO Insights – Survey' only				
Email	Email address	abc@company .com	Email is only applicable in VWO Insights - Surveys, and customers can choose not to collect it while using VWO as it is a question type within the survey feature. Survey can be run without email addresses as well. When Email collection is enabled in VWO surveys. Survey responses are encrypted by default.	Yes

[END OF ANNEXURE 1]

ANNEXURE 2: TECHNICAL AND OPERATIONAL SECURITY MEASURES

The security, integrity, privacy, and availability of your information are our top priorities. We know how vital it is to your business success. To ensure you never have to worry, we use a multi-layered approach to protect and monitor all your information.

1. Definitions. For the purposes of this Annexure 2:

1.1. "Application User" means any employee or personnel of the Customer who administers, configures, or otherwise uses VWO.

1.2. "VWO" means the VWO solution offered on a software as a service model by Wingify.

2. Information Security Program:

2.1. Wingify maintains a written information security program that:

(i) is managed by a senior employee responsible for overseeing and implementing the program.

(ii) includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity, availability, and privacy of Customer Account Data as required by Data Protection Law(s) and best practices.

(iii) is appropriate to the nature, size, and complexity of Wingify's business operations.

(iv) agrees to regularly test, assess and evaluate the effectiveness of its program to ensure the security of processing.

2.2. Wingify has comprehensive privacy and security assessments and certifications performed by third parties. Such certifications include ISO 27001:2013, ISO 27701:2019 standard certifications, details of which can be found at https://vwo.com/compliance/

3. Pseudonymization:

3.1. VWO does not collect nor does it require any Personal Data by default for its functioning.

3.2. VWO has also adopted a method where the UUID stored on the client-side is pseudonymized by using a one-way hash before storing it on its servers.

4. Anonymization:

4.1. Any IP address intended to be stored is stored with anonymization of at least the last octet (configurable by an Application User up to complete anonymization i.e. not storing it at all).

5. Application Security:

5.1. The VWO development team is trained on Open Web Application Security Project (OWASP) secure coding practices and uses industry best practices for building secure applications. Security team conducts whitebox testing on each code release and they also do a blackbox testing on third-party software to mitigate risk.

5.2. VWO code is stored in a code repository system hosted by our cloud data center provider. VWO adopts a strict, least access privileges principle for access to the code. Commits to production code are strictly reviewed and approved.

5.3. VWO production environment is logically segregated from the staging and development environment with concepts of virtual private cloud and subnets.

5.4. There is an hourly backup of the database data at secured cloud storage of cloud service provider.

5.5. All data flow in data pipelines (like recording, survey responses, and custom dimensions) is encrypted using a secure channel like TLS1.2. Data at rest is encrypted using AES 256 but standards (one of the strongest block ciphers available).

5.6. VWO has a password masking technique for the data lifecycle to ensure a secure key management process.

5.7. Connect to the VWO web-app via HTTPS by using the latest version of Transport Layer Socket (TLS) like TLS 1.2.

6. Application and System Access Control:

6.1. Role-based access and least access privileges principle provision while creating an account to ensure an appropriate level of access to the VWO account

6.2. Wingify access control mechanisms have the capability of detecting, logging, and reporting access to the system and application or attempts to breach security of the system or application.

6.3. Application Users have an individual account that authenticates that individual's access to Customer Account Data. Access controls including passwords are configured in accordance with industry standards and best practices.

6.4. Wingify maintains a process to review access controls on a minimum quarterly basis for all systems that transmit, process, or store Customer Account Data.

6.5. Wingify configures remote access to all systems and networks storing or transmitting Customer Account Data or Production environments to require multi-factors authentication for such access.

6.6. VWO supports Single Sign-On (SSO) through SAML 2.0.

6.7. Provision to restrict access to customer's VWO account to certain IP addresses

6.8. Provision to enable email alerts whenever specific activities take place in a customer's account.

6.9. Provision to sign out all other logged-in sessions

6.10. Provision to disable/delete application Users

6.11. Auto-logout of a application Users if the Password is changed in any other session or if the application Users is disabled/deleted

6.12. Session Management: Every time an application User signs in to the VWO account, the system assigns a new session identifier for the application User. The session identifier is a 64-byte random generated value to protect the account against brute force attacks. All sessions time out after 7 days, requiring the application User to sign in to their account again, and the currently active sessions are set to time out after 4 hours of inactivity. For best security, you can configure to terminate all sessions after 15minutes of inactivity.

7. Infrastructure and Network Security:

7.1. Wingify deploys firewall technology in the operation of the VWO's production environment. Traffic between Customer and VWO will be protected and authenticated by industry standard cryptographic technologies.

7.2. Wingify uses Google Cloud Security system which includes an Intrusion Detection System (IDS), a Security Incident Event Management (SIEM) system and other security monitoring tools on the production environment to generate, monitor, and respond to alerts which could indicate potential compromises of the system, network and/or application. Notifications from these tools are sent to the Wingify Security Team so that they can take appropriate action.

7.3. Wingify has implemented Open Source Host-based Intrusion Detection System (OSSEC) on our critical systems and regularly monitors them.

7.4. VWO regularly updates network architecture schemas and maintains an understanding of the data flows between its systems. Firewall rules and access restrictions are reviewed for appropriateness on a regular basis.

7.5. Access to VWO servers requires the use of a VPN with dual-factor authentication and extensive access monitoring.

8. Product Development and Maintenance:

8.1. Security by Design- Wingify applies security by design principles throughout the product development lifecycle, at the design and architecture level, by conducting security design review.

8.2. Open Source- Wingify evaluates and tracks vulnerabilities of open source software (OSS) and other 3rd party libraries that are incorporated into the VWO products. Wingify performs static code analysis and manual code review, as required by risk. Security verifications, including penetration testing and multiple dynamic analysis tools, are conducted by third-party firms, and security researchers.

8.3. Change Management- Wingify employs a documented change management program with respect to the products as an integral part of its security profile. This includes logically or physically separate environments from production for all development and testing.

8.4. Vulnerability Management and Application Security Assessments- Wingify runs internal and external network and system vulnerability scans at least quarterly and after any material change in the network and system configuration. Vulnerabilities identified and rated as critical and high risk are remediated or mitigated promptly after discovery.

8.5. For all internet-facing applications that process, transmit Customer Account Data, Wingify conducts an application security assessment review to identify common security vulnerabilities as identified by industry-recognized organizations (e.g., OWASP Top 10 vulnerabilities, CWE/SANS Top 25 vulnerabilities) annually or fall all major releases, whichever occurs first. The scope of assessment will primarily focus on application security, including, but not limited to, a penetration test of the application, as well as code review.

8.6. Wingify utilizes a qualified third party to conduct the application security assessments.

9. Storage, Handling and Disposal:

9.1. Data Segregation- Wingify logically separates and segregates Customer Account Data from its other Customer's data.

9.2. Encryption of Data- Wingify utilizes industry standard encryption algorithms and key strength to encrypt all Customer Account Data while in transit over all networks (e.g., Internet).

9.3. Destruction of Data- Customer Account Data is disposed of in a method that renders the data unrecoverable, to the extent reasonably possible, in accordance with industry best practices for wiping of electronic media (e.g. NIST SP 800-88).

10. Business Continuity and Disaster Recovery:

10.1. Wingify develops, implements, and maintains a business continuity management program to address the needs of the business, products and Services provided to the Customer. To that end, Wingify completes a minimum level of business impact analysis, crisis management, business continuity, and disaster recovery planning.

10.2. Wingify's business impact analysis plan includes, but is not limited to, a systematic review of business functions and their associated processes that identifies dependencies, evaluates potential impact from disruptions; defines recovery time objectives, and improves process understanding improvement, performed annually.

10.3. Wingify's Crisis management Plan includes, but is not limited to, elements such location workarounds, application work-arounds, vendor work-around, and staffing work-arounds, exercised at minimum annually.

10.4. Wingify's Disaster Recovery Plan includes, but is not limited to, infrastructures, technology, and system(s) details, recovery activities, and identifies the people/teams required for such recovery, exercised at least annually.

11. Operational Security:

11.1. VWO trains its employees to treat data protection and security as the highest priorities. VWO is committed to implementing tighter security standards across policies, procedures, technology, and people on an ongoing basis.

11.2. VWO runs Vulnerability Assessment Penetration Testing (VAPT) on an annual basis through a third-party service provider and performs quarterly security audits for all production environment systems.

11.3. Applications and servers are regularly patched to provide ongoing protection from exploits.

11.4. VWO has a disaster recovery strategy in place, which is tested on a half-yearly basis. Under any DR condition, our customer's websites will not get affected and will work fine. Though the data collection might get stopped until VWO services are restored, Uptime Status can be found at https://secure-stats.pingdom.com/yd4ybaf8hhh2.

11.5. Wingify follows the ISO 27001 control standard framework cross-reference with NIST SP 800-53 Rev 4, PCI DSS, CSA, SOC 2, HIPAA, GDPR, CCPA, etc.

12. Managing Privacy Protection Features:

12.1. VWO allows customers to turn on and off privacy impacting features to meet the applicable data protection law(s), details of which can be found at https://help.vwo.com/hc/en-us/articles/360019594533.

13. Multi-Tenancy:

13.1. All of VWO customer data is hosted in a secure cloud data center service provider and also logically segregated by the VWO application.

14. Due Diligence over Sub-Processors:

14.1. Wingify will conduct appropriate and commercially reasonable due diligence from an information security, privacy and legal perspective while engaging sub-processors.

14.2. Wingify will assess the security and privacy capabilities of any such sub-processors or vendors to adhere to Wingify's privacy and security evaluation, policies, and procedures.

14.3. Wingify will include written information security and compliance requirements that oblige sub-processors or vendors to adhere to Wingify key information security and privacy policies and standards consistent with and no less protective than these measures.

[END OF ANNEXURE 2]