

## Non-legalese, Simple English Summary

1. Your usage of our services will collect personal data of visitors of your website.
2. We will process data only as per your instructions.
3. You will be responsible for taking consent of your visitors.
4. We have taken technical and operational measures to protect personal data.
5. We will notify you within 48 hours in the event of a data breach.
6. For any query in data protection, you can reach our Data Protection Officer at [privacy@wingify.com](mailto:privacy@wingify.com).

## Data Protection Addendum

This Data Protection Addendum ("**Addendum**") is a part of the terms and conditions for use of VWO Service or other written or electronic agreement ("**Agreement**") between **Wingify Software Private Limited**

("Processor/Data Processor/Wingify"), a company registered under Indian Companies

Act, 1956, having its registered office at E-170, Antriksh Apartments, Sector-14, Rohini, Delhi-110085, India

*and*

the organisation using VWO ("**Controller**"),

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are added to the Agreement as amended by, and including, this Addendum.

### 1. Definitions

In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

**1.1. "Confidential Information"** Any information of whatever kind (whether technical, commercial, financial, operational, or otherwise) and in whatever form (whether oral, written, recorded, or otherwise), including Personal Data.

**1.2. "Data Processor"** means the Wingify Workforce entity that processes Personal Data on behalf of the Data Controller

**1.3. "Data Protection Laws"** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, and their member states, applicable to Processing of Personal Data under the Agreement.

**1.4. "GDPR"** means General Data Protection Regulation (EU) 2016/679); a legal framework regulation that sets guidelines for the collection and processing of personal information of living individuals within the European Union (EU), to strengthen and unify data protection.

**1.5. "Personal data"** means any information relating to an identified or identifiable natural person (**"Data Subject"**); an identifiable natural person is the one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, or online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

**1.6. "Processing"** means any operation or set of operations performed on Personal 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.)

**1.7. "Security Breach"** has the meaning given in Section 9 of this DPA.

**1.8. "Special categories of Data"** means racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited;

**1.9. "Services"** means the services and other activities to be supplied to or carried out by or on behalf of the Controller, pursuant to the Agreement;

**1.10. "Sub-processor"** means any person (including any third-party and any Processor Affiliate, but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor or any Processor Affiliate to process Personal Data on behalf of any Controller in connection with the Agreement;

The terms "Commission," "Data Subject," "Member State," "Personal Data Breach," "Processing," and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

## **2. Subject and Term**

In the course of providing Services to a Customer pursuant to the Agreement, Wingify may Process Personal Data on behalf of Customers. Wingify agrees to comply with the following provisions with respect to any Personal Data Processed for Customers in connection with the provision of the Services.

The purpose of this Addendum is to describe the work to be carried out by the Processor in relation with the Agreement. This Addendum forms an integral part of the Agreement hereof. This Addendum shall be deemed to take effect from the Effective Date and shall continue in full force and effect until the termination of the Agreement.

## **3. Scope of Work**

The purpose of collection, processing, and using Personal Data from the Controller is to provide the services, as described in the Agreement, which forms an integral part hereof. The transfer, processing, and use of Personal Data take place in a member state of the European

Economic area. Any data transfer to a third country requires prior approval from the Controller and is subject to compliance with the special requirements on transfers of personal data to countries outside the EU/EEA.

The processing of Personal Data by the Processor shall take place within the framework of this Addendum and only to the extent that the Controller has instructed the Processor to do so in relation to the Agreement. The Processor processes Personal Data on behalf of the Controller. Modifications to the processing of Personal Data under the Addendum are subject to mutual agreement. The Processor shall not use Personal Data for any other purpose, as described in this Addendum. The Controller shall not send any Special Category of Data to the Processor for processing.

The categories of data processed under this Addendum are mentioned in Appendix 1.

#### **4. Technical and Organisational Measures**

**4.1.** Wingify shall maintain administrative, physical, and technical safeguards for protection of security, confidentiality, and integrity of Personal Data. Such measures are set out in Appendix 2. Wingify monitors compliance with these safeguard measures.

**4.2.** Wingify has obtained third-party certifications and audits, as described in Wingify's Security Practices document. On Customers' written requests at reasonable intervals, Wingify shall provide a copy of Wingify's most recent third-party audits or certifications, as applicable, or any summaries thereof, that Wingify generally makes available to its customers at the time of such requests.

#### **5. Personnel**

**5.1.** Wingify shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of Personal 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.

**5.2.** Wingify shall take commercially reasonable steps to ensure the reliability of any Wingify personnel engaged in Processing of Personal Data.

**5.3.** Wingify shall ensure that Wingify workforce's access to Personal Data is limited to those personnel who require such access to perform an Agreement.

**5.4.** Data Protection Officer: Members of the Wingify Workforce have appointed a data protection officer where such appointment is required by Data Protection Laws. The appointed person be reached by email via [privacy@wingify.com](mailto:privacy@wingify.com).

#### **6. Processor Obligations**

Under this Addendum, the Processor has the obligation to:

- a. Process Personal Data only on behalf of the Controller and in compliance with its instructions, as mentioned in Annexure 1;
- b. Ensure that only appropriately trained personnel shall have access to Personal Data;
- c. Provide the Controller with such cooperation (including access to its facilities), as the Controller may reasonably request;

- d. Implement such technical and organizational measures to protect Personal Data, as required by the GDPR;
- e. Notify the Controller immediately over email of any monitoring activities and measures undertaken by the relevant authority that supervises the applicable data-protection legislation;
- f. Support the Controller regarding Controller's obligations to provide information about collection, processing, or usage of Personal Data to a data subject;
- g. Ensure that Personal Data is not used, manipulated, distributed, copied, or processed in any way other than the fulfilment of contractual obligations, as explicitly agreed upon and arising from this Addendum.

## 7. Sub-processing

The Controller agrees to the commissioning of the Sub-processors, as mentioned in Appendix 3, subject to a written agreement between the Processor and the Sub-processor with substantively the same obligations, as imposed on the Processor in this Addendum and the Agreement in accordance with the applicable data protection laws. Any such Sub-processors will be permitted to obtain Personal Data only to deliver the services Wingify has retained them to provide, and they are prohibited from using Personal Data for any other purpose.

The Processor shall not subcontract its obligations under this Addendum to a Sub-processor without the prior written consent of the Controller unless such Sub-processor undertakes, by way of a written agreement, substantially the same obligations, as imposed on the Processor in this Addendum and the Agreement. The Processor shall inform the controller of its intention to engage a Sub-processor. The Controller shall have the right to reasonably oppose the appointment of a new Sub-processor, within 10 days of receipt of information about the appointment/change of a Sub-processor, if the Controller shall have substantive and legitimate reasons for opposing the specific Sub-processor and shall notify the Processor of such objections in writing, as soon as possible, after receipt of the Processor's notice relating to such Sub-processor, failing which the appointment of the Sub-processor shall be deemed final. The addition or removal of a Sub-processor should not negatively affect the level of security within the Agreement to less than that which existed at the time of signing this Addendum.

## 8. Controller's rights and obligations

- a. Rights to monitor: The Controller is entitled to appoint a third-party-independent auditor who is in the possession of the required professional qualifications and is bound by a duty of confidentiality, which the auditor must be reasonably acceptable to the Processor, to inspect Processor's compliance with this Addendum and the applicable data protection legislation required to determine the truthfulness and completeness of the statements submitted by the Processor under this Addendum. The Controller's right to audit shall be subject to giving the Processor at least four weeks' prior written notice of any such audit at [privacy@wingify.com](mailto:privacy@wingify.com). These rights of the Controller shall not extend to facilities which are operated by Sub-processors which the Processor may use to attain its Purpose and provide its Services. The Processor shall ensure that the Processing activities carried out by any Sub-processors which the Processor may use to

attain its Purpose and provide its Services meet the requirements laid down in this Agreement and in applicable law.

- b. The Controller shall be responsible for obtaining consent for collection of personal data of Data Subjects which it will send to the Processor for processing.
- c. The Processor shall deal promptly and properly with all inquiries from the Controller relating to its processing of the personal data, subject to this Addendum.
- d. Rectification, deletion, and blocking of data: Upon instruction by the Controller through the VWO app, the Processor shall correct, rectify, or block Personal Data. Any request from a data subject directly to the Processor shall be directed to the Controller.

## 9. Security Breach Management and Notification

If the Processor cannot provide compliance or foresees that it cannot comply with its obligations, as set out in this Addendum, for whatever reasons, it agrees to promptly inform the Controller of its inability to comply, in which case the Controller is entitled to suspend the transfer of data. The Processor will promptly notify the Controller about:

- a. Any legally binding request for disclosure of Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
- b. Any accidental, unauthorised access, or other event that constitutes a personal data breach not later than forty-eight (48) hours after becoming aware of any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Personal Data;
- c. Any request received directly from the Personal Data subjects without responding to that request, unless it has been otherwise authorized to do so.
- d. Notification(s) of Security Breaches, if any, will be delivered to one or more of Customer's business, technical, or administrative contacts by any means Wingify selects, including through email. It is the Customer's sole responsibility to ensure that it maintains accurate contact information with Wingify at all times.
- e. An unsuccessful Security Breach attempt will not be subject to this Section. An unsuccessful Security Breach attempt is the one that results in no unauthorized access to Customer Personal Data or to any of Wingify's equipment or facilities storing Customer Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or servers, port scans, unsuccessful log-on and sign-in attempts, denial-of-service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers), or similar incidents; and
- f. Wingify's obligation to report or respond to a Security Breach under this Section is not and will not be construed as an acknowledgement by Wingify of any fault or liability with respect to the Security Breach.

The Processor shall indemnify the Controller for claims of any third-party that arise because of Processor's non-compliance with its obligations under this Addendum and the applicable local

laws and legislation of the countries where the Personal Data is processed and regulations regarding data protection and privacy.

Any and all written communications with respect to this Addendum shall only be addressed to the following persons (or to such other person as either Party may from time to time designate in writing):

For Controller: Organisation using VWO

Email: Work email provided at the time of sign-up

## 10. Deletion or Return of Personal Data

- a. The Processor shall promptly and in any event from 45 to 90 days of the date of termination/expiry of the Agreement return or, upon request, delete all Personal Data in accordance with Wingify's procedure and Data Protection laws and /or consistent within the terms of the agreement provided by the Controller.
- b. The Processor may retain Personal 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 Addendum will continue to apply for so long as the Personal Data provided by the Controller is Processed by the Contracted Processor.

## 11. Confidentiality


Confidential Information may be disclosed in any form or matter by one Party to the other Party, and with respect to, or as a result of this Addendum, it shall be deemed to be of a confidential nature. Data relating to Controller's customers database, procedures, and knowledge shall be considered private and confidential information.

## 12. Limitation of Liability

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this Addendum, 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 Agreement. The Processor's total liability for all claims from the Controller and all of its Authorized Affiliates arising out of or related to the Agreement and this Addendum shall apply in the aggregate for all claims under both the Agreement and the Addendum established under this Agreement.

The Processor shall not assign this Addendum without the prior written consent of the Controller. Where the Processor assigns this Addendum with the consent of the Controller, it shall do so only by way of a written agreement with the assignee which imposes the same obligations on the assignee as are imposed on the Processor under this Addendum.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out, as above.

|  |   |
|--|---|
| <p>On behalf of <b>Customer</b></p><br><br><br><p>Name:<br/>Title:<br/>Date:</p> | <p>On behalf of <b>Wingify Software Pvt. Ltd.</b></p><br><br><br><p>Name: Sparsh Gupta<br/>Title: Chief Executive Officer<br/>Date: July 25, 2018</p> |
|--|---|

### Appendix 1

#### Categories of Data to Be Processed

| Data Category                       | Data Element                   | Purpose  | Role of Wingify |
|-------------------------------------|--------------------------------|--|-----------------|
| Personally Identifiable Information | Country                        | When Post-Result Segmentation is turned on.  | Processor       |
| Personally Identifiable Information | Internet Protocol (IP) address | Anonymized IP address (with the last octet deleted) is stored when Post-Result Segmentation is turned on.  | Processor       |
| Personally Identifiable Information | Cookies                        | First-party cookies created to show the same variation of the tests to the visitor and to connect the journey across different features in VWO. A UUID is generated and stored on the browser, and a one-way hashed value is stored on VWO databases, or DBs (pseudonymization). | Processor       |
| Personally Identifiable Information | Custom Dimensions              | When Post-Result Segmentation is turned on or when the customer has configured it. VWO does not recommend sending any PII by using custom dimensions. There are measures to encrypt this data if any such PII is sent.   | Processor       |
| Personally Identifiable Information | Email                          | When Email collection is enabled in VWO surveys. Survey responses are encrypted by default.  | Processor       |

## Appendix 2

### Technical and Operational Measures

#### **Pseudonymization:**

- By default, VWO does not collect nor does it require any sensitive data for its functioning.
- VWO has also adopted a method where the UUID stored on the client side is pseudonymized by using a one-way hash before storing on its servers.

#### **Anonymization:**

- Any IP address intended to be stored is stored with anonymization of at least the last octet (configurable by a user up to complete anonymization).

#### **Application Security:**

- The VWO development team is trained on Open Web Security Application Project (OWASP) Secure Coding Practices and uses industry best practices for building secure apps.
- VWO code is stored on a code repository system hosted by our cloud data center provider. VWO adopts a strict, least access privileges principle for providing access to the code. Commits to production code are strictly reviewed, and approval is restricted to just Head of Engineering and Lead Engineers, after passing Unit Testing and QA in Test and Staging.
- The data stored on production servers is accessible only to the Head of Engineering and Lead Engineers. No other workforce member of VWO has access to customer data, unless access permission is granted by the Chief Executive Officer or the Head of Engineering to resolve any technical issue or for debugging.
- There is an hourly backup of the database data at our cloud data center provider.
- All data flow in data pipelines (like recordings, survey responses, and custom dimension) is encrypted by using the industry standard AES-256 encryption algorithm.
- Connect to the VWO web-app through HTTP or HTTPS by using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery. VWO application provides the option to enforce HTTPS-based usage.

#### **Application Access:**

- Role-based access and least access privileges principle provision while creating an account to ensure appropriate level of access to the VWO account
- Provision to restrict access to customer's VWO account to certain IP addresses
- Provision to enable email alerts in case of specific customer email account-related activities
- Provision to log off all other logged-on sessions
- Provision to disable/delete users





- Auto-logout of a user if the Password is changed in any other session or if the user is disabled/deleted

**Operational Security:**

- 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.
- Wingify follows the ISO 27001 standard framework. Wingify is ISO 27001:2013 (ISMS) and BS 10012:2017 (PIMS) certified.

**Multi-Tenancy:**

- All of VWO customer data is hosted on our cloud data center provider and is segregated logically by the VWO application.

**Appendix 3**

**Subcontractors to Be Used for Processing of Personal Data**

| Sub-Processor | Data Process  | Purpose                                      |
|---------------|---|--|
| IBM Softlayer | As per the customer configurations. Look at Appendix 1. | Provides infrastructure for running servers. |