Data Protection Addendum

PARTIES

Service Provider's Contracting Entity ("Provider")	As mentioned in the Agreement/Order Form
Service Provider Address	As mentioned in the Agreement/Order Form
Customer Contracting Entity ("Customer")	As mentioned in the Agreement/Order Form
Customer Address	As mentioned in the Agreement/Order Form

STANDARD CONTRACTUAL CLAUSES INFORMATION

For the purposes of the Standard Contractual Clauses:

Competent Supervisory Authority (as per Clause 13)	Based on the establishment of the Controller
Governing Law (as per Clause 17)	Based on the establishment of the Controller
Jurisdiction (as per Clause 18)	Based on the establishment of the Controller
Provider Contact Information	Name: Keshav Kumar Title: Data Protection Officer Contact: privacy@wingify.com
Customer Contact Information	As mentioned in the Agreement/Order Form

EXHIBITS

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

Exhibit 1	Categories of User Data
Exhibit 2	Technical and operational security measures
Exhibit 3	Standard Contractual Clauses

DPA TERMS AND CONDITIONS

INTERPRETATION

1. **Relationship with Agreement.** This DPA forms part of, and shall be co-terminus with the Agreement between the Customer and Provider. 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.

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

    1. **"Personal Data"** means any information related to any identified or identifiable natural person.

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

    3. **"Customer Account Data"** means any Personal Data other than User Data that is provided by the Customer or collected by Provider 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 Provider, 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.

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

    1. **"Data Protection Laws"** means the relevant and applicable data protection and data privacy laws, rules, and regulations applicable to Personal Data. Data Protection Law(s) shall include but not be limited to, the GDPR.

    2. **"Data Subjects"** shall have such meaning as provided under the GDPR.

    3. **"GDPR"** shall mean the Regulation (EU) 2016/679 of the European Parliament and the Council of 27th April 2016 on the protection of natural persons with regard to the processing of Personal data and on the free movement of such data, and repealing Directive 95/46/EC.

    4. **"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.

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

6. **"Services"** means the services provided to the Customer or any other activities performed on behalf of the Customer by Provider, pursuant to the Agreement.

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

8. **"Standard Contractual Clauses"** means: (i) the contractual clauses set out in Exhibit 3 for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of protection of Personal Data, which have been approved by the European Commission as adducing adequate safeguards for Restricted Transfers, or any successor clauses thereto or recognized by the European Commission pursuant to Article 46 of the GDPR, or by the relevant Secretary of State where the UK GDPR applies. Standard Contractual Clauses are referred to as "Clauses" within Exhibit 3, 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.

DATA PROCESSING

4. **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 Provider for Processing in the manner described in Exhibit 1. Provider shall ensure that sufficient technical measures are provided to enable the Customer to make such determination. Provider shall not Process any other User Data other than those specified in Exhibit 1.

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

6. **Customer Processing Instructions.** Provider 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 Exhibit 1). Provider 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 Provider to monitor and interpret the laws applicable to the Customer, and such notification will not constitute legal advice to the Customer.

   For User Data, Provider strictly acts as a Processor, processing such data only on the documented instructions of the Customer.

   For Customer Account Data, both parties act as independent Data Controllers, because each party independently determines the purposes and means of processing such data. Provider processes

Customer Account Data for purposes including, but not limited to: managing the contractual relationship with customers; account administration, billing, invoicing; support; internal business operations such as accounting, audits, taxation, and compliance; fraud prevention, abuse detection, security monitoring, and investigation of malicious activities; identity verification; compliance with legal and regulatory obligations; and other legitimate business purposes permitted under applicable privacy laws.

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

    1. Processing and storage necessary to provide the Services;

    2. to provide product support to the Customer; and/or

    3. disclosures as required by law or otherwise as set forth in the Agreement.

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

    1. to provide product support to the Customer; and/or

    2. disclosures as required by law, necessary to enforce any rights of Provider under the Agreement, or otherwise as set forth in the Agreement.

PROVIDER RESPONSIBILITIES

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

10. **Technical & Organisational Security Measures.** Provider 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 Exhibit 2. Provider monitors compliance with these safeguards. Customer acknowledges that such security & privacy measures are subject to technical progress and development and that Provider 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.

11. **Personnel.** Provider 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 Provider. Provider shall take commercially reasonable steps to ensure the reliability of any Provider personnel engaged in the Processing of User Data. Provider shall ensure that access to User Data and Personal Data is limited to those personnel who require such access to perform the Services.

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

SUB-PROCESSORS

13. Authorized Sub-Processors. Customer agrees that Provider may engage Sub-Processors to Process User Data on Customer's behalf or provide the Services as provided in https://wingify.com/compliance/subprocessors. For Customers purchasing, subscribing to, or otherwise using AB Tasty products and services, the sub-processors listed on AB Tasty's sub-processor page, available at https://www.abtasty.com/compliance-subprocessors/ , shall apply and are hereby incorporated by reference into this Agreement.

14. Obligations of Sub-Processors. Provider shall (i.) notify Customer at least 15 days in advance prior to onboarding any new sub-processor, providing Customer right to object within those 15 days (ii.) 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 (iii.) remain responsible for its compliance with the obligations of the DPA and for any acts or omissions of the Sub-processor that cause Provider to breach any of its obligations under this DPA.

CROSS-BORDER DATA TRANSFERS

15. **Location.** Unless the Customer has elected a different data hosting location or custom data residency arrangement in the applicable Order Form, Provider shall store and process User Data in the following default regions: (a) for Customers located in the European Economic Area ("EEA"), the United Kingdom, or Switzerland, User Data shall be stored in the EEA; (b) for Customers located in India, User Data shall be stored in India; and (c) for Customers located in the United States and all other jurisdictions not expressly covered under Sections (a) and (b), User Data shall be stored in the United States. Provider shall not intentionally store User Data outside the Customer's selected data hosting region, except where: (i) the Customer has provided prior written authorization or confirmation; (ii) the transfer is required by applicable law; or (iii.) following a customer reported issue, such transfer is necessary for the provision, security, support, or troubleshooting of the Services.

16. **European Commission Standard Contractual Clauses.** To the extent Provider 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. A copy of the Standard Contractual Clauses, as applicable currently, is attached hereto as Exhibit 3.

For the purposes of such Standard Contractual Clauses:

1. the Customer shall be the “Controller” and the “data exporter” and Provider shall be the “Processor” and the "data importer”;

2. the parties agree that Module Two (Controller to Processor) of the Standard Contractual Clauses shall be applicable;

3. Clause 9, Option 2 – General Written Authorization, with 15 days prior notice to Customer before onboarding any new sub-processor.

4. all references to “Annex I.A” shall instead refer to the information in this section and in page 1 of the DPA;

5. For the purposes of “Annex I.B”, the categories of Personal Data shall include any Customer Account Data and the purpose of Processing such data shall be limited to the extent required to provide the Services under the Agreement; and

6. all references to “Annex II.B”, shall instead refer to Exhibit 2 of this DPA.

CERTIFICATIONS AND AUDITS

17. **Certifications.** Provider has obtained privacy and security assessments and certifications by third parties, details of which can be found at https://wingify.com/compliance/ and https://trust.wingify.com/

18. **Records.** Provider 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.

19. **Reports and Audit.** Provider shall maintain records of its security standards. Upon Customer’s request, Provider 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 Provider’s compliance with this DPA. Provider 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 Provider’s compliance with this DPA.

20. **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.

    1. Customer is responsible for all costs and fees relating to such audit;

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

3. 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;

4. Such audit must not unreasonably interfere with Provider's business activities and must be reasonable in time and scope of Services;

5. 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

6. For any audit of any Sub-Processors, Provider shall endeavour to provide all commercially reasonable assistance to facilitate such audit.

INCIDENT RESPONSES AND COMMUNICATIONS

21. **Notice of Non-Compliance.** If Provider 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.

22. **Notice of Personal Data Breach.** Provider will notify Customer promptly and without undue delay (not later than 72 hours) 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. Provider'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 Provider recommends Customer take to address the Personal Data Breach.

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

24. **Data Subject Requests.** Any request from a data subject directly to Provider shall be directed to the Customer. Upon instruction by the Customer, Provider shall correct, rectify, or block any Customer Account Data to the extent they can be done by Provider. Provider 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 pursuant to Articles 12 to 22 GDPR, 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, Provider has no obligation to assess any Personal Data in order to identify information subject to any specific legal requirements.

25. **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 Provider's database, procedures, and processes shall be considered Confidential Information.

GENERATIVE AI USE AND OBLIGATIONS

26. The Customer acknowledges and agrees that the Services under this Agreement includes generative artificial intelligence ("GenAI") features. The Customer represents and warrants that any prompts, instructions, or other inputs provided by the Customer in connection with the GenAI features shall not infringe or misappropriate any third-party intellectual property, copyright, trademark, or other proprietary rights.

27. Where the Customer requests the generation of images or other creative content, the Customer shall ensure that such prompts do not reference, replicate, or otherwise include any protected or proprietary materials unless the Customer holds all necessary rights and permissions.

28. The Parties acknowledge that outputs generated by the AI features, including text, images, data, documents, code, or other materials ("Output"), are non-exclusive and non-proprietary and are not owned by either Party. No intellectual property rights in such Output are assigned or transferred to the Customer or Provider. The Customer may use the Output freely for its internal and commercial purposes, subject to applicable law and provided such use does not infringe third-party rights. Such use does not create or imply ownership of the Output or of the underlying AI systems, models, or technologies.

29. Provider does not reuse, or process any Personal Data for purposes other than providing the contracted services, and does not use such data for AI model training, or cross-customer use.

DISPOSAL AND RETENTION OF USER DATA

30. **Disposal of User Data.** Provider 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 Provider's procedure.

31. **Retention of User Data.** Provider 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.

LIABILITY

32. **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]

EXHIBIT 1: CATEGORIES OF USER DATA

Categories of User Data	Information stored by Provider's products	Examples	Nature and Purpose of Processing	Is it possible to identify data subject only 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	Provider 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. Provider 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 Provider.	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. This UUID is stored in Provider's serves solely as a pseudonymized identifier to distinguish browser sessions without linking it to personal attributes.	No
Additional Categories of Information to be Processed for 'Pulse - Surveys' only				

Email	Email address	abc@company.com	Email is only applicable in Pulse - Surveys, and customers can choose not to collect it while using Provider's products 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 Pulse-surveys. Survey responses are encrypted by default.	Yes
Phone number	Phone number	+1 9999999999	Phone number is only applicable in Pulse - Surveys, and customers can choose not to collect it while using Provider's products 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 Pulse-surveys. Survey responses are encrypted by default.	Yes

[END OF EXHIBIT 1]

EXHIBIT 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.

0. Definitions. For the purposes of this Exhibit 2:

1. "Application User" means any employee or personnel of the Customer who administers, configures, or otherwise uses Wingify, VWO and/or AB Tasty application.

2. "Wingify" or "VWO" means the Wingify or the VWO solution offered on a software as a service model by Provider.

3. "AB Tasty" means the AB Tasty solution offered on a software as a service model by Provider.

1. Information Security Program:

1. Provider maintains a written information security program that:

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

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

ii. is appropriate to the nature, size, and complexity of Provider's business operations.

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

2. The Provider has comprehensive privacy and security assessments and certifications performed by third parties. For Wingify/VWO products, such certifications include ISO 27001:2022 ISMS, ISO 27701:2019 PIMS standard certifications, SOC 2 Type II details of which can be found at https://wingify.com/compliance/ and https://trust.wingify.com/ and For AB Tasty products, such certifications include ISO 27001:2022 ISMS.

2. Pseudonymization:

1. The Provider stores only a randomly generated UUID as the cookie identifier. Under GDPR, pseudonymization means replacing identifiers with a value that cannot directly identify a person without additional information.

2. Since this UUID contains no fingerprinting data and only serves to distinguish browser sessions, it functions as a pseudonymized value rather than directly identifying personal data.

3. **Anonymization:**

    1. Complete IP addresses are never stored. Only anonymized IP addresses may be 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).

4. **Application Security:**

    1. The Provider 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.

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

    3. The Provider's production environment is logically segregated from the staging and development environment with concepts of virtual private cloud and subnets.

    4. For AB Tasty products, there is a daily backup of the database data and For Wingify products, there is an hourly backup of the database data at secured cloud storage of cloud service providers.

    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).

    6. Both Wingify and AB Tasty have a password masking technique for the data lifecycle to ensure a secure key management process.

    7. Connect to the Wingify and AB Tasty web-app via HTTPS by using TLS 1.2.

5. **Application and System Access Control:**

    1. Role-based access and least access privileges principle provision while creating an account to ensure an appropriate level of access to the Wingify and AB Tasty account.

    2. Provider 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.

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

4. Provider maintains a process to review access controls on a minimum quarterly basis for all systems and applications owned by Provider, involved in processing, transmitting or storing personal data.

5. Provider configures remote access to all systems and networks storing or transmitting User Data or Production environments to require multi-factors authentication for such access.

6. The provider supports Single Sign-On (SSO) through SAML 2.0.

7. Provision to disable/delete application Users

8. Below additional controls are only applicable for Wingify products:

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

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

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

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

    5. Session Management: Every time an application User signs in to the Wingify 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.

6. Infrastructure and Network Security:

1. The provider deploys firewall technology in the operation of the AB Tasty's and Wingify's production environment. Traffic between Customer and the Provider's application(s) will be protected and authenticated by industry standard cryptographic technologies.

2. For Wingify products, Provider 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 Provider Security Team so that they can take appropriate action and For AB Tasty products, the provider has implemented a SIEM solution, managed and handled by the Provider's in-house team.

3. For Wingify products, The provider has implemented Open Source Host-based Intrusion Detection System (OSSEC) on our critical systems and regularly monitors them.

4. The Provider 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.

5. Access to Provider's application(s) servers requires the use of dual-factor authentication and extensive access monitoring.

7. **Product Development and Maintenance:**

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

2. Open Source- Provider evaluates and tracks vulnerabilities of open source software (OSS) and other 3rd party libraries that are incorporated into the Provider's application(s)/products. Provider performs manual code review, as required by risk and for Wingify products, the Provider also performs static code analysis. Security verifications, including penetration testing are conducted by third-party firms, and security researchers.

3. Change Management- Provider 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.

4. Vulnerability Management and Application Security Assessments- Provider 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.

5. For all internet-facing applications that process, transmit User Data, Provider 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.

6. Provider utilizes a qualified third party to conduct the application security assessments.

8. **Storage, Handling and Disposal:**

1. Data Segregation- Provider logically separates and segregates User Data from its other Customer's data.

2. Encryption of Data- Provider utilizes industry standard encryption algorithms and key strength to encrypt all User Data while in transit over all networks (e.g., Internet).

3. Destruction of Data- User 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).

9. Business Continuity and Disaster Recovery:

1. Provider 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, Provider completes a minimum level of business impact analysis, crisis management, business continuity, and disaster recovery planning.

2. Provider'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.

3. Provider'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.

4. Provider'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.

10. Operational Security:

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

2. The provider runs Penetration Testing on an annual basis through a third-party service provider and performs regular security audits for all production environment systems.

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

4. For Wingify products, the provider has a disaster recovery strategy in place, which is tested on a 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 Wingify services are restored, Uptime Status for Wingify can be found at https://status.vwo.com/ ; https://status.wingify.com/ and for AB Tasty, Uptime status can be found at https://status.abtasty.com/

5. For AB Tasty products, Provider follows ISO 27001:2022 ISMS, GDPR, CCPA etc. and for Wingify/VWO products, Provider follows the ISO 27001:2022 ISMS control standard framework cross-reference with NIST SP 800-53 Rev 4, PCI DSS, CSA, SOC 2, HIPAA, GDPR, CCPA, etc.

11. Managing Privacy Protection Features:

1. For Wingify products, the Provider 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.

2. For Wingify/VWO Insights product, the Provider provide a complete guide on Navigating Data Protection Laws w.r.t Session Recordings and Safeguarding which are available at https://vwo.com/compliance/compliance-session-recordings/

3. Details on Role Based Access Control for Wingify Application Users is available at https://help.vwo.com/hc/en-us/articles/360019423094-Role-Based-Access-Control-for-VWO-Users

12. Multi-Tenancy:

1. All User data is hosted in a secure cloud data center service provider and also logically segregated by the Wingify and AB Tasty application.

13. Due Diligence over Sub-Processors:

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

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

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

[END OF EXHIBIT 2]

EXHIBIT 3: STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1: Purpose and Scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Clause 2: Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3: Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clauses 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clauses 9(a), (c), (d) and (e);

(iv) Clauses 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clauses Clause 18(a).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4: Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5: Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6: Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7: Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8: Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without

revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9: Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to

protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10: Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11: Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12: Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13: Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14: Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred

personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15: Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16: Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17: Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law as provided in page 1 of the DPA.

Clause 18: Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts as provided in page 1 of the DPA.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

[END OF EXHIBIT 3]