UserTesting Data Processing Agreement for Customers

This DPA governs any UserTesting Processing of Customer Personal Data on behalf of our Customers.

You (or "Customer") and UserTesting, Inc. and its Affiliates ("UserTesting") agree to the terms and conditions of this Data Processing Agreement, including the Standard Contractual Clauses, and its Appendices (collectively, the "DPA") in connection with your use of the UserTesting Platform and Services, as defined in and pursuant to our Agreement.

By accessing the Platform and using the Services, you agree to this DPA. This DPA supplements and is incorporated into the UserTesting Customer Terms and Conditions (as updated from time to time) (the "Terms") or other written agreement between us under which UserTesting agrees to provide you with access to the Platform and Services (the UserTesting Customer Terms and Conditions or such other agreement are referred to herein as the "Agreement").

If there is a conflict or inconsistency between this DPA and our Agreement, then the terms of this DPA will control. Any capitalized terms used but not defined in this DPA will have the meanings given to them in either the Agreement or the Applicable Laws, as further described below.

RECITALS

WHEREAS, UserTesting carries out cross-border transfers of data to and from the US and other locations, and Processes such data for the purpose of providing the Services to you, including storage of your Sessions and Recordings, storage of certain other information, support of security and threat analysis, billing, and account provisioning.

WHEREAS, Tests and Sessions are controlled by the Customer and the transmission to UserTesting of Customer Personal Data for Processing is determined solely by Customer.

WHEREAS, the Service is hosted by UserTesting's data center partners, which maintain independently validated security programs, including SOC 2 and ISO 27001, and our systems are regularly tested by independent third-party penetration testing firms to continually assess and improve our security posture; and

WHEREAS, UserTesting does not voluntarily permit US or other governmental agencies access to its infrastructure.

THEREFORE, for good and valuable consideration, the parties agree as follows:

AGREEMENT

1. Definitions. For the purposes of this DPA, “Commission", “Controller”, "Customer Personal Data Breach", "Member State", “Processor”, and "Supervisory Authority" shall have the meaning given in the European Union (EU) General Data Protection Regulation 2016/679 (“GDPR”) or any other Applicable Laws. “Business,” “Consumer” and “Service Provider,” shall have the meaning given in the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100, et seq. (“CCPA”). “Processing” (and its derivatives) has the meaning given to it in the GDPR or the CCPA, as the context of this DPA requires.

    1.1. “Affiliates” means any business entity that owns more than fifty percent (50%) of the voting interest in a party, or otherwise directly or indirectly controls, is controlled by, or is under common control with a party.

    1.2. "BCRs" means the binding corporate rules approved pursuant to Article 47 and 63 of the GDPR.

    1.3. “Applicable Laws” means any data protection laws applicable to UserTesting, including the GDPR, the UK GDPR and the CCPA.

    1.4. “Customer Personal Data" means “personal data" or “personal information” (as defined under Applicable Laws) that UserTesting obtains and Processes on Customer’s behalf, in the course of providing Services to Customer. For purposes of this DPA, Customer Personal Data does not include personal data or personal information that UserTesting obtains or Processes (i) from Contributors outside a Test or Session or (ii) independent of its Agreement with Customer.

    1.5. “Standard Contractual Clauses” or “SCCs” means the unmodified EU Standard Contractual Clauses for Processors pursuant to the European Commission Decision of 5 February 2010 for Customer Personal Data exported from the UK and Switzerland and the EU Standard Contractual Clauses for Processors pursuant to the European Commission Decision as of 4 June 2021 for Customer Personal Data exported from the EEA.

    1.6. “Subprocessor” (or “sub-processor”) has the meaning given in the SCCs.

    1.7. “Transfer” or “Transferred” means the transfer, disclosure, or other type of access to Customer Personal Data to a person, organization, or system located in a country or jurisdiction other than the country or jurisdiction where the Customer Personal Data originated.

    1.8. “UK GDPR” means the EU GDPR as amended and incorporated into UK law.

2. Roles, Purposes and Customer’s Instructions.

    2.1. Roles. In respect of any Customer Personal Data, Customer is the Controller or the Data Exporter under the GDPR and Business under the CCPA, UserTesting is the Processor or the Data Importer under the GDPR and Service Provider under the CCPA, and UserTesting’s sub-contractors are Subprocessors under the GDPR and Service Providers under the CCPA. UserTesting’s Processing of Customer Personal Data will

comply with SCCs. For the avoidance of doubt, UserTesting is the Controller and Business with respect to the personal data and personal information it collects directly from Contributors outside of a Test or Session, which is subject to the UserTesting Contributor Terms of Service and its Privacy Policy.

2.2. Purposes. UserTesting agrees that it will only collect and Process Customer Personal Data on Customer's behalf for the purposes of (i) providing and enhancing the Platform and Services, and (ii) detecting data security incidents and protecting against fraudulent or illegal activity. UserTesting will not Process Customer Personal Data for any other purpose without Customer's consent, including for the purpose of providing services to another person or entity. UserTesting will not sell Customer Personal Data.

2.3. Customer Instructions. UserTesting will conduct all Processing of Customer Personal Data in accordance with Customer's written instructions, which are deemed fully reflected in this DPA unless Customer and UserTesting specifically agree to additional written instructions (which will supplement, but not replace, the instructions in this DPA). UserTesting will promptly inform Customer of any instruction issued by Customer which, in its opinion, infringes Applicable Laws. Customer Personal Data (including business contact details of Customer's employees, agents and others whose data is collected or received in the course of carrying out this DPA and the Agreement) shall be Processed as reasonably required for the business relationship between the parties. Customer is responsible for ensuring any required data subject consent is duly provided, and UserTesting shall have no liability arising from the Processing of Customer Personal Data in accordance with Customer's written instructions. Customer will hold UserTesting harmless and indemnify UserTesting for any damages suffered or incurred due to UserTesting's Processing of Customer Personal Data in accordance with Customer's instructions. In accordance with Applicable Laws, UserTesting has implemented the technical and organizational measures listed under the attached Appendix Annex II, which are intended to protect Customer Personal Data against (i) unauthorized or accidental access or disclosure, (ii) misuse, (iii) corruption, and (iv) loss or destruction.

3. Request to Access Customer Personal Data. If a third party requests access to, or correction of, Customer Personal Data, UserTesting will refuse the request, and instruct the third party to make such request directly to Customer, and provide the third party with Customer's contact information. If compelled to disclose Customer Personal Data due to a legal demand by a law enforcement agency or other third party, UserTesting will give Customer notice of such demand before granting such access, to allow Customer to seek a protective order or other appropriate remedy. If notice to Customer is legally prohibited, UserTesting will use commercially reasonable efforts to protect the Customer Personal Data from undue disclosure, as if it were UserTesting Confidential Information being requested.

4. Customer Personal Data Breach. UserTesting will notify Customer without undue delay if it becomes aware of unauthorized or accidental access or misuse of the Customer Personal Data it Processes under the Agreement and will endeavor to mitigate the effects and to minimize any data protection breach. UserTesting will take action to prevent any further breach and provide Customer with all reasonable cooperation and assistance in relation to any notifications that Customer is required under Applicable Law to make as a result of said breach.

5. Transfer. You acknowledge and agree that we may access and Process Customer Personal Data on a global basis as necessary to provide the Services in accordance with the Agreement, and in particular that Customer Personal Data will be transferred to and Processed by UserTesting in the US and other jurisdictions where we, our Affiliates, and our Subprocessors have operations. We will ensure such transfers comply with the Applicable Laws. We will not transfer Customer Personal Data from the EU to any country or recipient not recognized as providing an adequate level of protection for Customer Personal Data unless we first take all necessary measures to ensure the transfer is in compliance with Applicable Laws. Such measures may include transferring such data to a recipient that (i) is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Customer Personal Data, (ii) has achieved BCRs, or (iii) has executed appropriate SCCs.

6. Obligations towards Subprocessors. Whether the Subprocessor is a UserTesting Affiliate or a third party, UserTesting will:

    6.1. restrict Subprocessors' access to Customer Personal Data to what is reasonably necessary to maintain or provide the Platform and Services to Customer;
    6.2. impose substantially similar appropriate contractual obligations in writing upon Subprocessors that are no less protective than the obligations set forth in this DPA; and
    6.3. remain responsible for Subprocessors' compliance and performance with the obligations of this DPA.

7. List of Subprocessors. UserTesting's Subprocessors include its Affiliates (as noted in Appendix - Annex III). Customer consents to UserTesting's use of its Affiliates and other Subprocessors in the provision of the Platform and Services. UserTesting will provide notification of new or changes in its Subprocessor(s) before authorizing any new Subprocessor(s) to Process Customer Personal Data under the Agreement. Where required by Applicable Laws, Customer may object to the engagement of any new Subprocessor but will not unreasonably withhold its consent to such appointment.

8. Audit. Subject to your confidentiality obligations, we will provide you with all information necessary to enable you to demonstrate compliance with Applicable Laws, and reasonably allow for and contribute to audits, including inspections by you or your auditor, to the extent such information is in our control and we are not precluded from providing it by applicable laws or contractual obligation to another party. You acknowledge that the Service is hosted by our data center partners who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are regularly tested by independent third-party penetration testing firms. Upon request, we will supply (on a confidential basis), (i) a summary copy of our most recent penetration testing report(s) to you so that you can verify our compliance with this DPA and (ii) responses to your reasonable requests for information, including responses to information security and audit questionnaires, to confirm UserTesting's compliance with this DPA and the GDPR. Customer acknowledges and agrees that it exercises its audit right under Clause 5(f) of the SCCs and under the GDPR by making requests under this clause.

    You will be solely responsible for any fees charged by any auditor you may appoint and for any damage, injury, or disruption to our premises, equipment, personnel, and business caused by your auditor. If a third party is to conduct the audit, the third party must be mutually agreed to by Customer and UserTesting and must execute a written confidentiality agreement with Customer and UserTesting before conducting the audit. To request an audit, Customer must submit to UserTesting a detailed audit plan at least two months in advance of the proposed audit date, describing the proposed scope, duration, and start date of the audit. UserTesting will review the

audit plan and notify Customer of any concerns or questions (for example, any request for information that could compromise UserTesting's security, privacy, employment, or other relevant policies). Both parties will work cooperatively to agree on a final audit plan, which may include charges for expenses incurred by UserTesting. If the requested audit scope is addressed in a similar audit report performed by a qualified third-party auditor within the prior twelve months and UserTesting confirms there are no material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report. Customer will provide UserTesting with any audit reports generated in connection with any audit under this section, unless prohibited by law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports are otherwise Confidential Information of the parties under the terms of the Agreement.

When reviewing our compliance with this DPA, you commit to take all reasonable measures to limit the impact on us and our Affiliates by combining several audit requests carried out on behalf of the Customer entity that is the contracting party to the Agreement and all of its Affiliates subject to the Agreement in one single audit and make such requests no more than once per year. Customer may perform more frequent audits to the extent required by Applicable Laws or upon specific request by a regulatory body.

9. Data Retention. UserTesting may delete Customer Personal Data after 12 months from the end of the provision of Services, or upon Customer's request as prescribed in the Agreement, unless UserTesting is required by law to retain a copy of Customer Personal Data.

10. Miscellaneous.

    10.1. Notwithstanding anything to the contrary, the parties acknowledge that the Applicable Laws are not intended to jeopardize or undermine the confidentiality obligations to which the parties are subject in the Agreement or an agreed upon non-disclosure agreement.

    10.2. Should any provision or condition of this DPA be held or declared invalid, unlawful, or unenforceable by a competent authority or court, then the remainder of this DPA will remain valid.

    10.3. This DPA will be effective for so long as our Agreement is effective. UserTesting may update its online terms with email notice to the Customer. Any other amendments to this DPA must be in writing and signed by authorized representatives of each party.

Schedules 1 and 2: Standard Contractual Clauses and International Data Transfer Addendum

Unless otherwise agreed in writing by the parties, by executing an Order, Customer is deemed to execute the SCCs as set out in full on our website, which will have legally binding force on the parties. A link to the SCCs can be found here. The following Appendices are incorporated by reference into the SCCs.

Appendix - ANNEX I to SCC 2021
(Appendix 1 to Schedule 1 to SCC 2010)

DESCRIPTION OF TRANSFERS

This Appendix - Annex I (or "Annex I") is incorporated into the DPA. All capitalized terms used but not defined below will have the meanings given to them in the DPA.

A. LIST OF PARTIES

Data Exporter
The Data Exporter is (i) the company that has executed the Standard Contractual Clauses as a Data Exporter and (ii) all Customer Affiliates (as defined under the Agreement) established within the European Economic Area (EEA) and Switzerland that export Customer Personal Data under the Agreement.

Data Importer
The Data Importer is UserTesting, Inc. and its Affiliates. The Data Importer provides the UserTesting Platform and Services to the Data Exporter under the Agreement, in the course of which it Processes certain Customer Personal Data as a Processor.

B. DESCRIPTION OF TRANSFER

Nature of the Processing
The Data Importer provides the Platform and Services to the Data Exporter, in the course of which it Processes certain Personal Data as a Processor. UserTesting Platform is software platform that enables its customers to develop test plans and define audiences in order to solicit perspectives on any brand, design, content or offering.
The data exporter's data on the UserTesting Platform will be hosted and stored in a 3rd party data center (AWS) in the US or EEA.

Purpose(s) of the data transfer and further processing
The Data Importer processes Customer Personal Data for the purposes of providing services to the Data Exporter in particular, delivering and making available to the Data Exporter, the records, recordings and analyses from interviews, surveys and sessions conducted on the UserTesting Platform.

Duration of processing, the period for which the personal data will be retained, and/or the criteria used to determine that period
Customer Personal Data is retained for the time period during which the data importer provides the Services to the data exporter until data is deleted upon Customer's request. In the absence of Customer's request for deletion, UserTesting may delete Customer Personal Data after 12 months from the end of the provision of Services, unless UserTesting is required by law to retain a copy of Customer Personal Data.

Data Subjects
The Customer Personal Data transferred concerns the following categories of data subjects:

- Employees, agents, and consultants of Customer
- Contributors, in Tests and Sessions

Categories of Data
The Customer Personal Data transferred concerns the following categories of data:

- Personal Data or other personally identifiable information included in responses to Tasks and questions included by Customer in a Test
- Face Recordings in Sessions designed to capture Face Recordings (consent is obtained before recording)
- Personal Data or other personally identifiable information inadvertently captured by screen and audio recordings

Sensitive Data Transferred

Customer may request special categories of information in a Test, such as any information about children or an individual's racial/ethnic origin, health, sexuality, political opinions, religious beliefs, criminal background or alleged offenses, or trade union membership, subject to the Customer's compliance with applicable laws and the Agreement.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data will be transferred on a continuous basis.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing

In the scope of providing the UserTesting Platform and Services, including technical support, UserTesting and its Subprocessors may need access to or process the personal data that is entered by data exporter into the UserTesting Platform in order to provide the subscription service. A list of Subprocessors used by UserTesting in effect as of the date of this DPA is included in Appendix - Annex III. A then-current list of UserTesting's Subprocessors is available at **https://www.usertesting.com/subprocessors**.

C. COMPETENT SUPERVISORY AUTHORITY

The supervisory authority of the Data Exporter.

Appendix - ANNEX II to SCC 2021

(Appendix 2 to Schedule 1 to SCC 2010)

Technical and Organizational Security Measures

This Appendix – Annex II (or "Annex II") is incorporated into the DPA and summarizes the technical, organizational, and physical security measures implemented by the parties. All defined terms not defined below will have the meanings given to them in the DPA.

UserTesting's Information Security is centrally managed by its Information Security team. The UserTesting Information Security team's responsibilities include the management of information security across all global locations, all UserTesting products and services and engagement of UserTesting Subprocessors.

In addition to any data security requirements set forth in the DPA, UserTesting will comply with the following:

1. Security Governance
    a. UserTesting's security policy is approved by its executive team and formally reviewed annually. It requires that all employees be trained on their responsibilities in protecting personal and confidential information. New employees are trained during orientation. All employees are required to refresh their training at least yearly.
    b. UserTesting has obtained SOC 2 Type 2 certification. The certification report is shared upon requests from customers and prospects (under NDA). UserTesting is also self-certified under Privacy Shield although we do not rely on Privacy Shield as a legal basis for transfers of Customer Personal Data.

2. Service Authentication
    a. Complex passwords are required for client and contributor access. Passwords must be at least 8 characters long and must contain at least one uppercase letter, one lowercase letter, and one digit. They may also contain special characters.
    b. Users are logged out of the system after periods of inactivity. The exact period is adjustable by account to meet individual customer requirements.
    c. When users create new accounts, they create their own secure passwords. When existing users create accounts for others, the new users are invited by email and are then asked to create their own secure passwords.
    d. Lost passwords are not retrievable but can be reset by the user by responding to an email sent to the account's email address that is already on record.
    e. Accounts are locked for 30 minutes if a user fails to supply a valid password 10 times in 30 minutes.

3. Single Sign-on
    UserTesting also supports login via single sign-on using SAML 2.0 protocols. This enables customers to implement additional security requirements for passwords and the login process.

4. Multi-factor authentication (MFA) for internal accounts
    UserTesting requires that internal email and development accounts use MFA.

5. Data Hosting and Encryption
    a. All confidential and proprietary data (including video files, Customer and Contributor data) are hosted through Amazon Web Services (AWS). AWS is a SOC 2 and ISO 27017 certified hosting provider.

b. All data is encrypted at rest and in transit. Data is stored in encrypted form using 256-bit AES encryption. Encryption keys are managed by AWS Key Management Services.
c. All communication to and from the data center is encrypted (TLS 1.2 or greater required).

6. Vulnerability Scanning
UserTesting performs quarterly vulnerability scans on infrastructure devices, servers, and user computers. Cloud infrastructure, virtual instances, web applications, and production code changes are scanning for vulnerabilities to ensure weaknesses are identified fast, and vulnerabilities remediated quickly.

7. Prototype, Image and Asset Hosting
UserTesting is able to host some web assets used during tests. The assets are encrypted at rest and only accessed through SSL. These are kept securely in our AWS infrastructure and only accessible through secure links that are inactive unless the test is in progress and used by the assigned, active contributor.

8. Data Lifecycle Management

Unless UserTesting is required by law to retain a copy of Customer Personal Data, UserTesting may delete Customer Personal Data one year after the end of the provision of Services. UserTesting will delete Customer Personal Data upon request from Customer.

9. Personnel Security
a. UserTesting conducts background checks on all employees, contractors, and consulting agencies, and does not hire individuals with inappropriate backgrounds.
b. Employees who leave the company or change business roles will have their access privileges revoked or modified within 24 hours.

10. Clean Desk Policy
UserTesting's clean desk policy mandates that employees keep all confidential information stored in a secure location and never left unattended in workspaces.

11. Facility Security
All UserTesting's office locations are secured by keycard locks that are assigned to individual employees and are monitored by video at all times. Visitors must sign in and be escorted at all times. Physical security audits are performed annually.

12. System Development
a. UserTesting builds its platform using an agile development methodology that releases small changes frequently after peer review and testing.
b. Every change that is built runs first on a local system. Changes are peer reviewed and then tested on non-production systems. After all tests are passed, and peer reviews completed, changes are deployed to the production system. Each change is processed by static analysis tools that look for known vulnerabilities in any component used. Tests are performed on separate systems (built the same way) but using seed data or obfuscated production data so that tests may be performed without risking the production system.
c. Deployment is managed by automated tools. The scripts that drive the tools are also kept under change control.
d. Virtual instances are checked nightly and critical software patches are applied as necessary.
e. Customer data is not used outside of production. Exceptions are made when troubleshooting issues where real data is relevant and even then the data is first obfuscated to prevent exposure of the personal information of Customers and Contributors.

13. Network and Device Security
a. UserTesting employs firewalls to protect our internal systems. Access to admin and hosting systems requires secure login to a centrally managed VPN.

b. Wireless access within the site requires corporate credentials. Other computers and mobile devices use an alternative access point that is outside the firewall.
c. Company-owned computers are managed and kept up-to-date with the latest operating system, antivirus, and productivity software updates.
d. BYOD (Bring your own device) are allowed in limited circumstances and computers must meet the above company standards to be used for business purposes.
e. All production systems are backed up to geographically diverse AWS data centers and securely stored in encrypted form.

14. Security Audits
UserTesting requires an annual, independent security audit of both internal systems and the platform. Copies of the most recent audit reports are available upon request.

15. Logging
System activity is centrally logged. Logs are kept for a minimum of 12 months in ways that make them virtually impossible to tamper with.

16. Intrusion Detection, Prevention and Incident Response
System accesses are monitored and logged. ThreatStack software is deployed on every instance in the VPC and alerts when it encounters unusual activity. Custom monitors look for other unusual activity. Alerts are investigated by engineers according to an incident response plan. The plan is designed to effectively escalate incidents to the appropriate level of authority, ensuring quick fixes that are followed up with a root cause analysis and work plan, to prevent future incidents. The incident response plan is reviewed annually.

17. Web Application Firewall (WAF)
UserTesting employs a WAF implemented using AWS WAF platform to prevent certain kinds of common attacks. AWS automatically updates the managed rules as new exploits and bad actors emerge.

18. Data Loss Prevention (DLP)
UserTesting deploys DLP tools on company workstations to track and alert when unusual activity is detected. Additional DLP tools are deployed in critical cloud infrastructure.

19. Subprocessors
UserTesting uses a number of third parties to deliver its full platform of services. Most do not have access to confidential information. Any that do are subject to annual security reviews and are obligated by contract to provide a security posture that is at least as stringent as what we provide directly.

20. Business Continuity
Business continuity is included as part of UserTesting's security policy. The platform has been designed to be robust and recoverable.
- The platform is hosted on multiple servers running in AWS with load balancing and failover provisions
- Instances can be spun up as needed if one fails
- Videos are stored in journaled S3 buckets
- Videos are stored in at least two geographically-diverse data centers
- Other data is stored in RDS with continuous backups to alternate data centers and daily snapshots.
- Data centers are located in geographically-diverse locations to ensure redundancy in the case of a catastrophic event

Appendix ANNEX III to SCC 2021

Sub-processors and Subsidiaries

This Appendix – Annex III is incorporated into the DPA.

The full list of the subprocessors can be found at: https://www.usertesting.com/usertesting-subprocessors

Last updated: February 7, 2022

‘