Data Processing Agreement

This Data Processing Agreement, including any schedules attached to it (hereinafter, the "**DPA**"), supplements the Terms of Service available at https://www.requestly.com/terms, unless Customer has executed a written Master Software Subscription Agreement (MSSA) for such Services, in which case the MSSA will govern (hereinafter, the "**Agreement**") for using **Requestly Services,** entered into by and between the Customer, as defined in the Agreement, hereinafter, the "**Controller**") and **BrowserStack. Inc,** including its affiliates (hereinafter, the "**Processor**"), a Delaware corporation having its registered office at 4512 Legacy Dr., Suite 100 Plano, TX 75024. By executing the Agreement, the Controller enters this DPA on behalf of itself and, to the extent required under applicable Data Protection Legislation (as defined below).

Controller and Processor are hereinafter individually referred to as a "**Party**" and collectively referred to as the "**Parties**".

WHEREAS:

1. Controller and Processor have exchanged the necessary documentation, including without limitation privacy policies, terms of service, records of processing activities, and information and security policies, for the Parties to be able to frame the actions to be undertaken under the present DPA; and

2. Controller and Processor wish to lay down in this DPA the assignment for and further agreements concerning the processing of this Personal Data by Processor under or in connection with the Agreement.

IT IS AGREED AS FOLLOWS:

1. INTERPRETATION

1.1 In this DPA, the following words shall have the hereinafter stated meaning when written with a capital letter:

- **Agreement:** has the meaning given to that term in the recitals of this DPA.
- **Appropriate Technical and Organisational Measures:** has the meaning given to such term in Data Protection Legislation (including, as appropriate, the measures referred to in Article 32(1) of the GDPR).
- **Approved Sub-Processors:** means the Sub-Processors that have been approved by the Controller in accordance with Section 5.
- **Data Protection Legislation:** means applicable laws and regulations relating to the privacy and security of Personal Information, including but not limited to GDPR and the Data Protection Acts 1988 to 2018 of Ireland,and to privacy including the E-Privacy Directive 2002/58/EC and the

European Communities (ElectronicCommunications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ("E-Privacy Regulations") of Ireland, as such laws shall be supplemented, amended, revised or replaced from time to time

- **Personal Data Breach:** means any "personal data breach" as defined in the GDPR in respect of the Personal Information of the Users which is caused while using the Services
- **Controller:** has the meaning given to such term in Data Protection Legislation.
- **Processor:** has the meaning given to such a term in Data Protection Legislation.
- **Data Subjects:** means the individual using Requestly Services to whom Personal Information pertains;
- **Personal Information:** means the Personal Information of the User that Processor or any Approved Sub-Processor will process when providing the Services to the Controller. For the purpose of this definition, "processing" of Personal Information and "Personal Information" will have the meaning given to those terms under the applicable Data Protection Legislation.
- **Privacy Manager**: Means the contact person appointed by the Processor for all data protection matters;
- **Restricted Transfer**: any transfer of Personal Information in Account-Related Personal Information to countries outside of the EEA which are not subject to an adequacy decision by the European Commission, where such transfer would be prohibited by Data Protection Legislation.
- **Services:** means the services that Processor will provide to Controller under or in connection with the Agreement.
- **Standard Contractual Clauses**: the contractual clauses dealing with the transfer of Personal Information outside the EEA, which have been approved by (i) the European Commission under Data Protection Legislation, or (ii) by a competent supervisory authority under Data Protection Legislation, available here.

1.2 If there is any conflict or inconsistency between any:

1.2.1 term in the main part of this DPA;

1.2.2 term in any of the schedules to this DPA; and

1.2.3 term in the Agreement and its schedules and annexes;

the term falling into the category first appearing in the list above shall take precedence.

2. GENERAL OBLIGATIONS

2.1 When processing Personal Information, the Parties will always comply with their obligations under all applicable Data Protection Legislation.

2.2 Processor will agree to comply with any Appropriate Technical and Organisational Measures as attached to this DPA as Attachment 1.

2.3 Processor will (and will ensure that the Approved Sub-Processors will) only process Personal Information on behalf of the Controller:

2.3.1 in the manner and for the purposes set out in Schedule 1, including any of its sub-schedules; and

2.3.2 upon the written instruction of the Controller.

2.4 In addition to the foregoing, the Controller hereby:

2.4.1 instructs Processor to take such steps in the processing of Personal Information on behalf of the Controller as are reasonably necessary for the provision of the Services under or in connection with the Agreement; and

2.4.2 authorizes Processor to provide to the Approved Sub-Processors and on behalf of Controller instructions that are equivalent to the instructions set out in Section 2.4.1.

2.5 The Controller represents and warrants that the documentation it provides to Processor in connection to this DPA for the delineation of its tasks under same agreement, therein included, without limitation its privacy policies and its safety and security policies, are true and accurate on the date as of which such information is provided to Processor in the light of the circumstances and purposes for which such documentation has been provided.

2.6 If in Processor' reasonable opinion, compliance with Controller's instructions would constitute a breach of the applicable Data Protection Legislation, Processor will promptly notify Controller thereon in writing within a reasonable delay.

1. If the Controller does not answer to Processor' reasonable opinion referred above, within a delay of fourteen (14) calendar days of receiving it, Processor will be free to put the particular instruction aside, without incurring any penalty or liability in that regard. If the Controller should persist in its instruction, and the Processor remains unsatisfied, the Parties agree to enter mutual discussions and address the matter, and, if required, contact the relevant authority pursuant to common decision of both Parties.

3. CONFIDENTIALITY AND SECURITY

3.1 Processor undertakes to treat all Personal Information strictly confidential. Unless Controller requires otherwise in writing, Processor will not disclose Personal Information to any third party other than:

3.1.1 to those of its employees, Approved Sub-Processors, and employees of the Approved Sub-Processors to whom such disclosure is strictly necessary for the provision of the Services, provided that:

(i) any disclosure under this Section 3.1.1 is made subject to strict obligations of confidentiality and data protection no less onerous than those imposed upon Processor under this DPA, under the Agreement, and consistent with any procedures specified by Controller from time to time;

(ii) the persons to whom Personal Information may be disclosed pursuant to Section 3.1.1 will have received appropriate training regarding the data protection obligations that Processor and the Approved Sub-Processors must comply with under applicable Data Protection Legislation and under this DPA;

(iii) Processor will implement measures to ensure that any persons to whom Personal Information may be disclosed pursuant to Section 3.1.1 will not process Personal Information except on instruction from the Controller; or

3.2.2 to the extent required by law, by any governmental or other regulatory authority, or by a court or other authority of competent jurisdiction, provided that Processor will:

(i) give written notice to Controller of any disclosure of Personal Data that Processor or any Approved Sub-Processor is required to make under Section 3.1.1, promptly after it becomes aware of that requirement (unless such notice is prohibited by applicable legislation); and

(ii) co-operate with Controller regarding the timing and content of such disclosure and any action which Controller may wish to take to challenge the validity of such requirement.

3.2 In regard to the Controller, the Processor will (and will ensure that the Approved Sub-Processors will) implement the necessary security measures and will keep these measures in place for the entire term of this DPA.

4. REPORTING DATA SECURITY INCIDENTS

4.1 Processor shall, without undue delay, inform Controller if any of Personal Information is lost or destroyed or becomes damaged, corrupted, or unusable, or if there is any accidental, unauthorised or unlawful disclosure of or access to any of Personal Information. In such case, Processor will use commercially reasonable efforts to restore Personal Information at Controller's expense (except where the incident was caused by Processor's negligent act or omission, in which case it will be at Processor expense), and will comply with all of its obligations (if any) under Data Protection Legislation in this regard.

4.2 The processor must inform the Controller of any Personal Data Breaches, or any complaint, notice or communication in relation to a Personal Data Breach, without undue delay. Taking into account the nature of Processor's processing of the Personal Information available to Processor and at Controller cost Processor will provide sufficient information and assist Controller in ensuring compliance with Controller's obligations in relation to notification of Personal Data Breaches (including the obligation to notify Personal Data Breaches to the applicable supervisory authority within seventy two (72) hours), and communication of Personal Data Breaches to Data Subjects where the breach is likely to result in a high

risk to the rights of such Data Subjects. Taking into account the nature of Processor's Processing of the Personal Information and the information available to Processor and at Controller cost, Processor shall co-operate with Controller and take such reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

5. SUBCONTRACTING AND SUB-PROCESSING

5.1 Processors may add or replace a sub-processor, and the same shall reflect in the list of Sub-Processors as given under Schedule 1. In case of objection by the Controller to such addition or replacement, The Controller shall communicate the same objection to the Processor via Email. In the absence of such an objection, the sub-processor will be considered an Approved Sub-Processor.

5.2 Processor and the Sub-Processor will enter into a written data processing agreement setting out the same, considered functionally rather than formally, (or more onerous) obligations as those set out in this DPA.

5.3 For the purpose of Section 5.1, the Controller hereby accepts the subcontracting of the processing of Personal Data to the Sub-Processors described in Schedule 1. The Sub-Processors described in this link will be deemed to be the Approved Sub-Processors for the purpose of this DPA.

5.4 The Processor will not be liable for acts and omissions of the Approved Sub-Processors unless the same was foreseeable to the Processor.

6. AUDIT

6.1 Processor Audits: The Processor uses external auditors to verify the adequacy of its security measures. This audit: (a) will be performed at least annually; (b) will be performed according to relevant standards; (c) will be performed by independent third party security professionals at Processor's selection and expense; and (d) will result in the generation of System and Organization Controls (SOC) 2 Report ("Report"), which will be Processor's Confidential Information.

6.2 Audit Reports: At Controller's written request, and provided that the parties have an applicable NDA in place, Processor will provide Controller with a copy of the Report and other documents and information via questionnaires, so that Controller can reasonably verify Processor's compliance with its obligations under this DPA.

6.3 The Controller agrees to exercise any right it may have to conduct an audit or inspection, under the Standard Contractual Clauses if they apply, by instructing the Processor to carry out the audit described in Section 6.a. If the Controller wishes to change this instruction regarding the audit, then the Controller has the right to request a change to this instruction by sending the Processor a written notice as provided for in the Agreement. If a written notice is sent by the Controller, including under the Standard Contract Clauses if they apply, Processor will allow Controller or an independent auditor appointed by Controller to conduct audits once every five (5) years, if required by law and in accordance with this Section:

- The Controller must send a written request for audits to the Processor.
- Following receipt by Processor of such request, Processor and Controller shall discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of the SOC 2 report; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit.
- The Controller shall be solely responsible for any and all costs / expenses pertaining to such an audit.
- Processor may object in writing to an auditor appointed by the Controller to conduct any audit if the auditor is, in Processor's reasonable opinion, not suitably qualified or independent, a competitor of Processor, or otherwise manifestly unsuitable. Any such objection by the Processor will require the Controller to appoint another auditor or conduct the audit itself.
  If Processor declines to follow any instruction requested by Controller regarding audits or inspections, Controller is entitled to terminate this DPA and the Agreement.If the Standard Contractual Clauses apply, except for providing clarification on their implementation, nothing in this Section varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or Data Subject's rights under the Standard Contractual Clauses.

7. ASSISTANCE WHEN HANDLING REQUESTS FROM DATA SUBJECTS

7.1. Processor will (and will ensure that the Approved Sub-Processors will) fully cooperate with Controller when handling requests from Data Subjects exercising their rights, including (without limitation) their right to be informed about the processing of their Personal Data, under applicable Data Protection Legislation.

7.2. Processor shall:

7.1.1 without undue delay notify the Controller when Processor (or any Approved Sub-Processors) receives a request from a Data Subject under any of the applicable Data Protection Legislation in respect of the Personal Data; and

7.1.2 take all required actions and provide all required information, by e-mail to the Privacy Manager or by letter to the address of the Processor as indicated above within fifteen (15) days as of its receipt, unless otherwise instructed by the Controller; and

7.1.3 ensures that it (or any Approved Sub-Processor) does not respond to that request except on the documented instructions of Controller or as required by applicable Data Protection Legislation to which Processor is subject.

8. **Restricted transfers**

8.1 A Restricted Transfer may not be made by Processor (other than transfers to Processor's Affiliates and by any agents and contractors for the purposes of performing the Services, and Controller shall use commercially reasonable efforts to obtain explicit consent from relevant Data Subjects in respect of such potential transfers) without the prior written consent of Controller (such consent not to be unreasonably withheld, delayed or conditioned), and if such consent has been obtained (or is unnecessary), such

Restricted Transfer may only be made where there are Appropriate Safeguards in place with regard to the rights of Data Subjects (including but not limited to the Standard Contractual Clauses, binding corporate rules, or any other model clauses or transfer mechanism approved by the applicable supervisory authority).

8.2 Subject to Clause 8.5, in the event of any Restricted Transfer by Processor to a contracted Sub-processor, to any Affiliate of Controller or otherwise ("Data Importer") for which Controller's consent has been obtained (or is unnecessary), Processor and Controller shall ensure that (i) Controller (where the RestrictedTransfer is being made at the request of Controller) or Processor acting as agent for and on behalf of Controller (where the Restricted Transfer is being made at the request of Processor), and (ii) the DataImporter, shall enter into the Standard Contractual Clauses in respect of such Restricted Transfer. The Party who is entering into the Standard Contractual Clauses with a Data Importer shall comply with the guidance of any relevant regulatory authority on Restricted Transfers in particular with respect to the use of Standard Contractual Clauses and any additional measures required to be taken in the context of any such Restricted Transfers.

8.3 Subject to Clause 8.5, any Restricted Transfer made by one Party ("Data Exporter") to the other Party ("Data Importer") shall be made subject to the provisions set out in the Standard Contractual Clauses contained here, and such Standard Contractual Clauses (except for any optional provisions contained in same, which shall not apply) are hereby specifically incorporated into this Agreement by reference for such purpose.

8.4 Subject to Clause 8.5, in the event that a transfer of Personal Data from the EEA to the United Kingdom is considered a Restricted Transfer, because the United Kingdom has left the European Union, Parties shall procure that the Data Importer shall enter into the Standard Contractual Clauses in respect of such Restricted Transfer.

8.5 Clauses 8.1 or 8.2 shall not apply to a Restricted Transfer if other compliance steps (which may include, but shall not be limited to, obtaining explicit consents from Data Subjects) have been taken to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Legislation.

8.6 In the event that there is any conflict between the Standard Contractual clauses and the other provisions of this Agreement, such Standard Contractual Clauses shall take precedence in respect of such conflict (other than in respect of legislative references etc. which have been updated pursuant to Data Protection Legislation since the date of approval of such Standard Contractual Clauses.)

9. TERM AND TERMINATION

9.1 This DPA enters into force on its signature and will remain in force as long as the Processor will provide the Services under the Agreement unless this DPA is terminated earlier in accordance with this Section 10.

9.2 The Controller has the right, without prejudice to its other rights or remedies, to terminate this DPA immediately (without the necessity for judicial action) by written notice to Processor if the latter is in material breach of this DPA and either that breach is not capable of remedy or, if the breach is capable of remedy, Processor has failed to remedy the breach within thirty (30) days after receiving written notice of default from Controller requiring it to do so.

9.3 Notwithstanding any other breach which qualifies as material under Section 8.2, any breaches by Processor of Sections 2, 3, 4, or 5, will be considered a material breach allowing Controller to terminate this DPA in accordance with Section 9.2.

10. RETURN/DESTRUCTION OF PERSONAL DATA

Upon termination or expiry of this Agreement, at the choice of Controller, the Processor shall delete or return all Personal Information and delete existing copies of the Personal Information, unless legally required/entitled to store Personal Information for a period of time. If the Controller makes no such election within a ten (10) days period of termination or expiry of this Agreement, BrowserStack may delete any any Personal Information in the Processors's possession; and if Controller elects for destruction rather than return of Personal Information, Processor shall as soon as reasonably practicable ensure that all Personal Information is deleted, unless legally required/entitled to store Personal Information for a period of time. The Personal Information will be deleted in accordance with the applicable product data retention policies as may be in place and amended or replaced from time to time.

11. APPLICABLE LAW AND JURISDICTION

This Agreement will be governed by the laws of California. US Courts will have exclusive jurisdiction for any dispute between the Parties arising out of or relating to this DPA.

Attachment 1

DESCRIPTION OF TECHNICAL AND ORGANISATIONAL MEASURES TAKEN BY THE PROCESSOR AND DESCRIPTION OF THE LOCATION OF DATA PROCESSING

The data processing is based in the US and the legal entity of the Processor incorporated in Delaware.

All the Personal Information are stored in a Firebase server in the United States. For encryption, the Processor uses https in transit and the hashing process at rest.

Google Firebase data centers feature state of the art environmental security controls to safeguard against fires, power loss, and adverse weather conditions. Physical access to these facilities is highly restricted, and they are monitored by professional security personnel.

Processor's offices are equipped with access control, intrusion detection, and video surveillance systems. All communications are encrypted over SSL/TLS 1.2, which cannot be viewed by a third party and is the same level of encryption used by banks and financial institutions.

Processor monitors documented threats from public security research databases (such as the Common Vulnerabilities and Exposures catalog), and its employees run automated vulnerability scanners, including retire.js and nsp, at regular intervals and before each deployment.

Processor's developers receive training for secure software development, including Open Web Application Security Project guidelines.

All major code changes are subject to a multipoint code review, with specific attention paid to security.

Processor maintains firewalls on its edge servers and origin load balancers to protect against bandwidth and protocol-based attacks, and Processor uses intelligent web application firewalls and elastic scaling of its compute capacity to mitigate attacks at the application layer, including complex and evolving attacks. All Personal Information is stored with at least dual redundancy, and Processor have designed its storage solution for 99% long-term durability.

Processor's team access is controlled by a carefully managed and audited security policy. All team members sign non-disclosure agreements to protect the user's Personal Information. All employees receive tools and training for handling sensitive data (including credentials) and for avoiding social engineering and other non-technical attacks.

Processor's team log activity across its platform, from individual API requests to infrastructure configuration changes. Logs are aggregated for monitoring, analysis, and anomaly detection and archived in vaulted storage. Processor implements measures to detect and prevent log tampering or interruptions.

Processor conducts regular internal security audits and reviews its hardware, software, and physical security configurations. If the Processor discovers a vulnerability, a formal incident response framework will be followed to ensure rapid mitigation and transparent Controller communication.

SCHEDULE 1: DESCRIPTION OF DATA PROCESSING

1. **Nature of Data**
   The nature of the Personal Information used is precisely defined in the Agreement.
2. **Categories of Data Subjects**
   The Categories of Data Subjects are precisely defined in the Agreement.
3. **The purposes of the data processing**
   The Personal Information will be processed to perform the Services as agreed in the Agreement and to manage the contractual relationship between the Processor and the Controller.
4. **The processing instructions**
   The processing instructions are set in the Agreement.
5. **The data protection officer or other contact person at the Controller:**
   The contact details are set in the Controller's privacy policy.
6. **The Privacy Manager at the Processor:**
   https://privacy.requestly.io/
7. **Approved Sub-Processors:**
   https://privacy.requestly.io/