Last Update: January 21, 2022

Data Processing Addendum (DPA)

This Data Processing Addendum ("**DPA**") forms part of the applicable master services or subscription agreement, including the Redis Enterprise Cloud Terms of Service (the "**Agreement**") by and between Redis Ltd., Redis EMEA Ltd., or Redis Inc. (as applicable) ("**Redis**") and the entity or organization whose details were provided in the signup process, applicable order form, or otherwise has an Agreement referencing this DPA (referred to as **"Customer"**) (Redis and Customer are, collectively, the "**Parties**"). All capitalized terms not defined herein will have the meaning set forth in the Agreement.

Background

In order to provide service(s) to Customer pursuant to the Agreement (the "**Service(s)**"), Redis may be required to store, retrieve, or perform other operations related to, or on personal data on behalf of Customer (see Processing definition below), based on Customer's instructions. This DPA is intended to reflect the Parties' agreement on the Processing of Personal Data under applicable Privacy Laws and Regulations (defined below).

1 DEFINITIONS

1.1 "**Affiliate**" means any legal entity directly or indirectly controlling, controlled by or under common control with a party to the Agreement, where "control" means the ownership of a majority share of the voting stock, equity, or voting interests of such entity.

1.2 **"CCPA"** means the California Consumer Privacy Act of 2018 and implementing regulations.

1.3 **"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.4 **"Customer"** means the entity using the Services that has executed an Agreement or applicable order form, which references this DPA.

1.5 **"GDPR"** collectively refers to Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 and Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 as it forms part of United Kingdom (UK) law by virtue of the European Union (Withdrawal) Act 2018.

1.6 "**Individual**" means a natural person to whom Personal Data relates, also referred to as **"Data Subject"** pursuant to the GDPR and similar Privacy Laws and Regulations.

1.7 "**Personal Data**" means information about an identified or identifiable Individual, also referred to as "**Personal Information,**" (or other substantially similar term) pursuant to applicable Privacy Laws and Regulations, which Redis Processes under the terms of the Agreement.

1.8 "**Personnel**" means the employees, agents, consultants, and contractors of Customer and Customer's Affiliates.

1.9 "**Privacy Laws and Regulations**" means all laws, statutes, regulations, and binding obligations applicable to the Processing of Personal Data under the Agreement, including, where applicable, the GDPR, CCPA, and the UK Data Protection Act 2018.

1.10 "**Process**", "**Processed**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.11 "**Standard Contractual Clauses**" or "**SCCs**" mean the standard contractual clauses for the transfer of personal data to third countries pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, which are available at this link.

1.12 **"Subprocessor(s)"** refers to a third-party service provider(s) that may need to Process Personal Information in the performance of the Service(s) on Customer's behalf. The list of applicable Subprocessors is available at this link, or by visiting https://redis.com/legal (the **"Redis Subprocessor List"**). Customer can also obtain a copy of the Redis Subprocessor List by submitting a support ticket.

2 DATA PROCESSING

2.1 **Scope and Roles**. This DPA applies when Personal Data is Processed by Redis as part of Redis provision of the Service, as further specified in the Agreement and the applicable order form. In this context:

(i) to the extent that the GDPR or other Privacy Laws and Regulations with analogous terms apply to Redis' Processing of Personal Data on behalf of Customer under the Agreement, Redis and applicable Affiliates are the Processor to Customer, who can act either as the controller or processor of Personal Data, as those or analogous terms are defined under applicable Privacy Laws and Regulations; and

(ii) to the extent that the CCPA applies to Redis Processing of Personal Data on behalf of Customer under the Agreement, (a) Customer is the "**Business**" and Redis and applicable Affiliates are the "**Service Provider**" as those terms are defined under the CCPA; (b) Redis will Process Personal Data solely on behalf of Customer and for the specific business purposes set forth in the Agreement; and (c) Redis will not retain, use, disclose, or otherwise Process such Personal Data for any purpose other than for the specific purpose of performing the Service as specified in the Agreement.

2.2 **Instructions for Redis' Processing of Personal Data**. Redis will only Process Personal Data on behalf of and in accordance with Customer's documented instructions including concerning transfers of Personal Data to a third country, unless Redis is required to otherwise Process Personal Data by applicable Privacy Laws and Regulations; in such case, Redis shall inform Customer of that legal requirement before Processing, unless that legal requirement prohibits such information on important grounds of public interest. Redis will promptly inform the Customer if, in its opinion, an instruction infringes applicable Privacy Laws and Regulations.

Customer hereby instructs Redis to Process Personal Data for the following business purposes:

(i) Processing in accordance with the Agreement and applicable order forms, including, without limitation to provide the Service, and for support, back-up and disaster recovery, cyber security, service operations and control, fraud and service misuse prevention and legal and administrative proceedings; and

(ii) Processing to comply with other reasonable instructions provided by Customer, where such instructions are consistent with the terms of the Agreement and comply with applicable Privacy Laws and Regulations; and

(iii) Processing outside the scope of this DPA (if any) will require prior written agreement between Redis and Customer on additional instructions for Processing, including agreement on any additional fees Customer will pay to Redis for carrying out such instructions.

2.3 **Subject Matter and Duration**. The subject matter and duration of the Processing under this DPA is for the purposes and duration of the Agreement. The nature and purpose of the Processing and the type of Personal Data and categories of Data Subjects about whom Personal Data shall be processed are determined by Customer, based on Customer's use of the Services and the Personal Data that Customer chooses to upload to the Service(s) or otherwise provide to Redis for the purpose of Processing. The categories of Data Subjects may include Customer's employees, staff, vendors, end users, or the Personal Data of any other Individuals whom Customer chooses to provide to Redis under the Agreement.

3 NOTICE, CONSENT, AND LAWFUL BASIS

3.1 Customer undertakes to provide all necessary notices to Individuals and receive all necessary permissions and consents and otherwise address any obligations related to the lawful basis for Processing as necessary for Redis to Process Personal Data on Customer's behalf under the terms of the Agreement and this DPA, pursuant to the applicable Privacy Laws and Regulations.

3.2 To the extent required under the applicable Privacy Laws and Regulations, Customer will appropriately document the Individuals' notices and consents or other lawful bases on which such Personal Data is Processed.

4 RIGHTS OF INDIVIDUALS

4.1 **Requests**. Redis will, to the extent legally permitted, promptly notify Customer if Redis receives a request from an Individual, whose Personal Data is included in Customer's Personal Data, or a request by the Individual's legal guardians, to exercise the right to access, correct, amend, or delete Personal Data related to the Individual, or to exercise such other personal right that the Individual is entitled to pursuant the applicable Privacy Laws and Regulations.

4.2 **Assistance**. Taking into account the nature of Processing by Redis and insofar that this is possible, Redis will provide Customer with cooperation and assistance in relation to handling Individuals' requests pursuant to applicable Privacy Laws and Regulations, by providing Customer with access to Customer's Data for the purpose of exercising the applicable individuals' rights. Except if not permitted under the applicable Privacy Laws and Regulations, Customer will reimburse Redis with any costs and expenses related to Redis' provision of such assistance, except for negligible costs.

4.3 **Accuracy of Personal Data.** Due to the nature of the Processing, Customer acknowledges and agrees that it is unlikely for Redis to become aware that Personal Data processed is inaccurate. If Redis becomes aware that Customer Data is inaccurate, it will inform Customer. Redis will cooperate with Customer to erase or rectify inaccurate Personal Data.

5 ASSISTANCE IN COMPLIANCE

5.1 At Customer's written request, Redis will assist Customer in complying with Customer's obligations pursuant to Articles 32 to 36 to the GDPR (or other substantially similar obligations under applicable

Privacy Laws and Regulations), in relation to the Processing of Customer's Personal Data by Redis, taking into account the nature of Processing and the information available to Redis.

6 REDIS PERSONNEL

6.1 **Limitation of Access**. Redis will ensure that Redis' access to Personal Data is limited to those personnel who require such access to perform the Agreement.

6.2 **Confidentiality**. Redis will impose appropriate contractual obligations upon its Personnel engaged in the Processing of Personal Data, including relevant obligations regarding confidentiality, data protection, and data security. Redis will ensure that its Personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training in their responsibilities, and are subject to appropriate confidentiality obligations .

7 AFFILIATES AND THIRD-PARTY SERVICE PROVIDERS

7.1 **Affiliates**. Some or all of Redis' obligations under the Agreement may be performed by Redis Affiliates.

7.2 **Subprocessors**. Customer acknowledges and agrees that Redis and Redis' Affiliates respectively may engage Subprocessor(s) in the performance of the Service(s) on Customer's behalf. All Affiliates and Subprocessors to whom Redis transfers Personal Data to provide the Service on behalf of Customer have entered into written agreements with Redis or such other instruments that bind them by substantially the same material obligations under this DPA.

7.3 **Liability**. Redis will be liable for the acts and omissions of its Affiliates and Subprocessors to the same extent that Redis would be liable if performing the Service of each Affiliate or Subprocessor directly, under the terms of the Agreement.

7.4 **Objection**. To ensure compliance with applicable Privacy Laws and Regulations, Customer may object to any engagement by Redis with a new Subprocessor to Process Customer Personal Data on Customer's behalf, within ten (10) business days following Redis' updating the online list of Subprocessors or otherwise providing notice to Customer of its engagement with the new Subprocessor. Customer agrees that any objection will be based on a reasonable and detailed reason. If Customer sends Redis a written objection to the new Subprocessor in accordance with the provisions of this section, Redis will make commercially reasonable efforts to provide Customer the same level of Service without using the new Subprocessor to Process Customer Personal Data. Nothing in this section prejudices the Parties' rights and obligations under the Agreement.

8 ONWARD AND CROSS-BORDER TRANSFER

8.1 **Transfer to Subprocessors.** All Redis' Subprocessors: (i) are subject to appropriate contractual safeguards (such as the Standard Contractual Clauses); (ii) have executed or undertaken to comply with such other binding instruments, certifications or self-certifications for the lawful transfer of Customer's Personal Data within the European Economic Area, the United Kingdom, or Switzerland to other territories, as required and available under the GDPR or other applicable Privacy Laws and Regulations; or (iii) are established in a country that was acknowledged by the EU Commission or applicable competent authority as providing adequate protection to Personal Data.

8.2 **Location of Data.** Customer may choose to have data hosted in different geographic locations when configuring the Services. If Customer configures the Services in such a way that Personal Data must be transferred between one geographic region to another, the following will apply (as applicable):

8.2.1 **Generally.** Where (i) Customer transfers Personal Data within the European Economic Area, the United Kingdom, or Switzerland to Redis (where such transfer includes Personal Data subject to the GDPR), and (ii) Redis will be Processing such Personal Data in a country that (a) is not subject to an adequacy decision of the EU Commission and (b) does not provide an adequate level of protection within the meaning of applicable Privacy Laws and Regulations, Attachment 1 to this DPA will apply.

8.2.2 **United Kingdom; Switzerland.** Attachment 2 to this DPA applies to the extent that the Customer is within the territorial scope of the applicable Privacy Laws and Regulations of either the United Kingdom or Switzerland.

8.2.3 **Israel.** Transfers of Personal Data within the EU to Israel, to the extent applicable, are made in accordance with the EU Commission decision 2011/61/EU of January 31, 2011, on the adequate protection of Personal Data by the State of Israel regarding automated processing of Personal Data.

8.2.4 **Adequacy Decision.** If the European Commission adopts a new adequacy decision, determining on the basis of Article 45 of the GDPR, that a jurisdiction outside of the EU offers an adequate level of protection, and such decision is published to the European Commission's website at this link, Redis and Customer agree that this decision may be used as a transfer mechanism for the applicable jurisdiction.

9 INFORMATION SECURITY

9.1 **Controls**. Redis will maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Customer's Personal Data based on industry standard information security measures (**"TOMs"**). Redis will regularly review and monitor compliance with these TOMs. The TOMs will, taking into account the nature, scope, context, and purposes of the Processing activities, be designed to protect against unauthorized or unlawful Processing, alteration, accidental destruction, or unauthorized access or disclosure of Personal Data. No material decrease in the overall security of the TOMs for the Service(s) will occur during the term of the Agreement. The TOMs can be requested by following the applicable support process or retrieved from https://redis.com/legal/.

9.2 **Policies and Audits**. Redis uses external auditors to verify the adequacy of its security measures. The internal controls of the Service are subject to periodic testing by such auditors. Upon Customer's written request at reasonable intervals and subject to confidentiality limitations, Redis will make available to Customer (or to a third-party auditor on Customer's behalf, that is not a Redis competitor and subject to the auditor's execution of Redis' non-disclosure agreement), the then most recent version of Redis' summaries of third-party audit or certification reports. Customer may conduct an audit of Redis' compliance with its obligations under this DPA up to once (1) per year (**"Data Protection and Security Audit"**), provided, however, that any Data Protection and Security Audit is subject to the following cumulative conditions:

(i) The Data Protection and Security Audit will be pre-scheduled in writing with Redis, at least sixty (60) days in advance;

(ii) All Customer personnel who perform the Data Protection and Security Audit, whether employed or contracted by Customer, will execute Redis' non-disclosure agreement prior to the initiation of the Data Protection and Security Audit, and a third-party auditor will also execute a non-competition undertaking;

(iii) Customer will take all necessary measures and verify that the auditors do not access, disclose or compromise the confidentiality and security of non-Customer data on Redis' information and network systems;

(iv) Customer will take all measures to prevent any damage or interference with Redis and its Affiliates' information and network systems, and to prevent any unreasonable interference with the day-to-day business operations of Redis;

(v) Customer will bear all costs and assume responsibility and liability for the Data Protection and Security Audit and for any failures or damage caused as a result thereof;

(vi) Customer will keep the Data Protection and Security Audit results in strict confidentiality, will use them solely for the specific purposes of the Data Protection and Security Audit under this section, will not use the results for any other purpose, or share them with any third party, without Redis' prior explicit written confirmation; and

(vii) If Customer is required to disclose the Data Protection and Security Audit results to a competent authority, Customer will first provide Redis with a prior written notice, explaining the details and necessity of the disclosure, and will provide Redis with all necessary assistance to prevent the disclosure thereof.

9.3 **Customer Configurations.** The Redis Enterprise Cloud Services and Redis Enterprise Software have configurable security options and settings that should be configured by Customer according to the Redis Enterprise security best practices documentation (**"Redis Security Configuration Best Practices"**). The Redis Security Configuration Best Practices for the Redis Enterprise Cloud Services is available at this link, and for Redis Enterprise Software the Redis Security Best Practices are available at this link. Customer agrees and understands that it has been provided with, and is aware of the Redis Security Configuration Best Practices.

10 SECURITY BREACH MANAGEMENT AND NOTIFICATION

10.1 **Breach Prevention and Management**. Redis will maintain security incident management policies and procedures and will, to the extent required by applicable law, promptly notify Customer of any unauthorized access to, acquisition of, or disclosure of Customer Personal Data, by Redis, its Affiliates or Personnel of which Redis becomes aware of (a "**Security Incident**").

10.2 **Remediation**. Redis will promptly make reasonable efforts to identify and remediate the cause of such a Security Incident.

11 DELETION AND RETENTION OF PERSONAL DATA

11.1 **Data Deletion**. Redis will provide Customer with the ability to remove Customer Personal Data and any copies of the same, during the term of the Agreement or upon or after the termination of the

Agreement. By providing such ability, Customer acknowledges that Redis fulfills the data deletion requirement under applicable Privacy Laws and Regulations.

11.2 **Data Retention**. Notwithstanding the above, Customer acknowledges and agrees that Redis may retain copies of certain records, log files and transactional details, as necessary in connection with its routine backup and archiving procedures and to ensure compliance with its legal obligations and its continuing obligations under applicable law, including to retain data pursuant to legal requirements and to use such data to protect Redis, its Affiliates, Personnel, and any person on their behalf in court and administrative proceedings.

12 DISCLOSURE TO COMPETENT AUTHORITIES

12.1 Redis may disclose Personal Data if required by law or a subpoena or other judicial or administrative order or if Redis deems the disclosure necessary to protect the safety and rights of any person, or the general public.

12.2 Redis undertakes to adopt supplementary measures to protect the Personal Data transferred under the SCCs (whether from the EU, UK, Switzerland or other jurisdiction requiring such supplementary measures) by the Data Exporter (**"SCC personal data"**), in accordance with the requirements of applicable Privacy Laws and Regulations, including by implementing appropriate technical and organizational safeguards, such as encryption or similar technologies, access controls or other compensating controls, to protect SCC personal data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense and public security.

12.3 In the event that Redis receives a legally binding request for access to the Personal Data by a public authority, Redis will:

(i) promptly notify Customer of such request to enable Customer to intervene and seek relief from such disclosure, unless Redis is otherwise prohibited from providing such notice. If Redis is so prohibited:

a. It will use its reasonable efforts to obtain the right to waive this prohibition, to communicate as much information as it can, and be able to demonstrate that it did so.

b. In the event that, despite having used its reasonable efforts, Redis is not permitted to notify Customer, it will make available general information, on an annual basis, and as allowed by law (such as a transfer impact assessment or other transparency report), concerning the requests it received to the Customer and/or the competent supervisory authority of the Customer.

(ii) comply with Redis internal policies governing the disclosure of Personal Data in response to requests from public authorities that conform to this DPA;

(iii) not make any disclosures of the Personal Data, to any public authority, that are determined to be massive, disproportionate, and indiscriminate in a manner that it would go beyond what is necessary in a democratic society; and

(iv) upon request from the Customer, provide general information on the requests from public authorities it received in the preceding twelve (12) month period relating to the Personal Data.

13 TERM

13.1 This DPA will commence on the same date that the Agreement is effective and will continue until the Agreement is expired or terminated, pursuant to the terms therein.

14 COMPLIANCE

14.1 Redis' Data Protection Officer and Redis' Compliance team are responsible for ensuring that all relevant Redis' personnel adhere to this DPA. Redis' Data Protection Officer can be reached at: privacy@redis.com.

15 DISPUTE RESOLUTION

15.1 Each Party will create an escalation process and provide a written copy to the other Party within five (5) business days of any dispute arising out of or relating to this DPA. The escalation process will be used to address disputed issues related to the performance of this DPA, including but not limited to, technical problems. The Parties agree to communicate regularly about any open issues or process problems that require prompt and accurate resolution as set forth in their respective escalation process documentation. The Parties will attempt in good faith to resolve any dispute arising out of or relating to this DPA, before and as a prior condition for commencing legal proceedings of any kind, first as set forth above in the escalation process and next by negotiation between executives who have authority to settle the controversy and who at a higher level of management than the persons with direct responsibility for administration of this DPA. Any Party may give the other Party written notice of any dispute not resolved in the normal course of business. Within two (2) business days after delivery of the notice, the receiving Party shall submit to the other a written response. The notice and the response will include (a) a statement of each Party's position and a summary of arguments supporting that position and (b) the name and title of the executive who will represent that Party and of any other person who will accompany the executive. Within five (5) business days after delivery of the disputing Party's notice, the executives of both Parties shall meet at a mutually acceptable time and place, including telephonically or videographically, and thereafter as often as they reasonably deem necessary, to attempt to resolve the dispute. All reasonable requests for information made by one Party to the other will be honored. All negotiations pursuant to this clause are confidential and will be treated as compromise and settlement negotiations for purposes of applicable rules of evidence.

16 MISCELLANEOUS

16.1 Invalidation by law or court review of one or more of the provisions under this DPA will not affect the remaining provisions. Invalid provisions will be replaced to the extent possible by those valid provisions which achieve essentially the same objectives.

16.2 All terms under the Agreement apply to this DPA, except that the terms of this DPA will supersede any conflicting terms under the Agreement. If there is any conflict between the SCCs and the Agreement (including this DPA), the SCCs shall prevail, to the extent the conflict relates to the processing of Customer Personal Data. Any claims against Redis under this DPA shall only be brought by the Customer entity that is a party to the Agreement against the Redis entity that is a party to the Agreement. In no event shall this DPA or any party restrict or limit the rights of any Data Subject or of any competent supervisory authority. Any limitations of liability in the Agreement will apply to this DPA to the fullest extent allowed by law.

Contents of this DPA :

- **Data Processing Addendum** - General Terms
- **Attachment 1** - General Data Transfer Provisions
- **Attachment 2** - Specific Data Transfer Provisions

ATTACHMENT 1 BEGINS ON NEXT PAGE

ATTACHMENT 1 TO REDIS DATA PROCESSING ADDENDUM (DPA)

GENERAL DATA TRANSFER PROVISIONS

1 DEFINITIONS

1.1 **Generally.** For purposes of these Data Transfer Provisions in this Attachment 1 to the Data Processing Addendum, the following definitions shall apply:

1.2 **"Data Exporter"** means Customer and any of its Affiliates and subsidiaries that transfer Customer Personal Data to Data Importer for the purposes specified in the Agreement.

1.3 **"Data Importer"** means Redis and any of its Affiliates, Personnel and Subprocessors that will have access to or otherwise process Customer Personal Data, in circumstances where the Personal Data originates from a data subject located in the country at issue, and is processed by Redis, its Affiliate, Personnel or sub-processor outside of that country.

1.4 **"Standard Contractual Clauses"** includes, for purposes of this Attachment 1, both *MODULE TWO: Transfer controller to processor* (**"Module 2"**) and, if applicable, *MODULE THREE: Transfer processor to processor* (**"Module 3"**) (referred to jointly as the **"Modules"**) of the Standard Contractual Clauses, as approved by the European Commission and as updated from time to time.

2 PROCESSING DETAILS

2.1 **Generally.** The following provisions apply to all transfers of Personal Data pertaining to Data Subjects located in the European Economic Area, from Data Exporter to Data Importer under this Agreement.

2.2 **Modules.** Module 2 will apply in the event that Customer is the controller of the Personal Data being Processed. In the event that Redis is a subprocessor on behalf of Customer as a Processor, Module 3 will apply.

2.3 This Section of this Attachment 1 describes the "*Activities relevant to the data transferred under these Clauses*" contained in the Modules:

2.3.1 The subject matter, nature, categories, and types of Personal Data subject to Processing or transfer are described in Section 2.3 of the DPA above. Further, the descriptions of scope and transfer, described in Section 2 of the DPA above, shall compromise the Description of Transfer for the purposes of Annex I.B of the Appendix of the Standard Contractual Clauses.

2.3.2 The duration of the Processing activities are continuous until the lapse or termination of the Agreement.

2.3.3 The purpose of the Processing is the provision of the Service(s) to Customer.

2.4 The details contained in the Redis Subprocessor List are agreed by the Parties to constitute a description of transfers to applicable Subprocessors. From time to time, Redis may add Subprocessors to this list by providing an update to amend this Support Policy in its sole discretion. Redis will post the amended terms on the Redis website.

3 AMENDMENTS TO THE MODULES

3.1 Module 2 and Module 3 are hereby amended as follows, to the extent allowed by applicable law:

3.1.1 Any Clause purporting to allow the admission of contracting parties without mutually executed signed writings will not apply (including but not limited to any optional docking clauses); and

3.1.2 The parties agree that this Agreement and DPA are based on the General Written Authorisation concepts relating to subprocessors, and the specified time period for informing the Controller of any intended changes in the subprocessor list is five (5) days in advance, and any optional language requiring Prior Specific Written Authorisation will not apply, except in the case of a mutually executed amendment between Controller and Processor; and

3.1.3 Any audit right described in Module 2 or Module 3 shall be satisfied by the audit procedures explicitly described in this DPA, except to the extent officially mandated by Privacy Laws and Regulations; and

3.1.4 The Optional language of Clause 11 will not apply; and

3.1.5 The first Option in Clause 17 will apply, except as otherwise described in this Attachment 1 or in Attachment 2, and the Standard Contractual Clauses will be governed by the law of the Republic of Ireland; and

3.1.6 In Annex I(A) of the Appendix the Data Importer's "Name"; "Address"; "Contact person's name, position and contact details" shall be those details of Redis as defined in this Agreement; and

3.1.7 In Annex I (C) of the Appendix: (i) the competent supervisory authority shall be drafted as the supervisory authority which is competent to supervise the activities of the Data Exporter or, (ii) where the Data Exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the Data Subjects relevant to the transfer are located.

End of Attachment 1

ATTACHMENT 2 TO REDIS DATA PROCESSING ADDENDUM (DPA)

SPECIFIC DATA TRANSFER PROVISIONS

In the event Personal Data is to be transferred out of the United Kingdom or Switzerland, as described in the DPA, the following shall apply:

1.1 References to the Standard Contractual Clauses, or the law of the EU, will have the meaning given to them by the equivalent Privacy Laws and Regulations of the United Kingdom (the **"UK"**), and Switzerland.

1.2 With respect to the processing of Personal Data to which the UK Data Protection Act 2018, as amended, applies, the competent supervisory authority is the Information Commissioner's Office; and with respect to the processing of Personal Data to which the Swiss data protection laws apply, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

1.3 In the event that, and to the extent applicable, the definition of Personal Data is more expansive under the Privacy Laws and Regulations of Switzerland, and such additional data is to be protected as if it were Personal Data from an Individual, then the definition of Personal Data will be expanded to include this.

1.4 If the Data Exporter is subject to the territorial jurisdiction of the UK, or the Data Exporter is established under the laws of the UK, then the UK will have exclusive jurisdiction to resolve disputes arising out of the Standard Contractual Clauses.

1.5 If an Individual who's Personal Data is being Processed under the terms of this DPA is a permanent resident of Switzerland, then the Swiss courts will be available as a venue, and with jurisdiction, to resolve disputes arising out of the Standard Contractual Clauses.