Google Cloud Backup and DR Data Processing and Security Terms

These Data Processing and Security Terms, including their appendices (the "Terms") are incorporated into the agreement under which Actifio has agreed to provide Google Cloud Backup and DR (as described at https://console.cloud.google.com/tos?id=backupdr) and related technical support to Customer (the "Agreement")

1. Commencement

These Data Processing and Security Terms (the "Terms") will be effective and replace any previously applicable data processing and security terms as from the Agreement Effective Date.

2. Definitions

In these Terms:

"Additional Security Controls" means security resources, features, functionality and/or controls that Customer may use at its option and/or as it determines, including encryption, security scanning, and firewalls.

"Adequate Country" means:

(a) for data processed subject to the EU GDPR: the EEA, or a country or territory that is the subject of an adequacy decision by the Commission under Article 45(1) of the EU GDPR;

(b) for data processed subject to the UK GDPR: the UK or a country or territory that is the subject of the adequacy regulations under Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018; and/or

(c) for data processed subject to the Swiss FDPA: Switzerland, or a country or territory that (i) is included in the list of the states whose legislation ensures an adequate level of protection as published by the Swiss Federal Data Protection and Information Commissioner, or (ii) is the subject of an adequacy decision by the Swiss Federal Council under the Swiss FDPA.

"Alternative Transfer Solution" means a solution, other than the Model Contract Clauses, that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Law.

"Customer Personal Data" means the personal data contained within the Customer Data.

"Data Incident" means a breach of Actifio's security leading to the accidental or unlawful

destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Actifio.

“EEA” means the European Economic Area.

“Full Activation Date” means the date the Customer accepted this Agreement.

“EU GDPR” means 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, and repealing Directive 95/46/EC.

“European Data Protection Law” means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

“European or National Law" means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); and/or (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data).

“GDPR” means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.

“Model Contract Clauses” or “MCCs” mean the standard data protection clauses (MCC EU Controller-to-Processor and MCC UK Controller-to-Processor, as applicable), which are incorporated by reference into these Terms, for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the EU GDPR and the UK GDPR, respectively.

“MCC EU Controller-to-Processor” means terms at https://docs.actifio.com/Actifio-GO/PDFs/Actifio-C2P-Standard-Contract-Clauses-EU-Data-Transfers.pdf

“MCC UK Controller-to-Processor” means terms at https://docs.actifio.com/Actifio-GO/PDFs/Actifio-C2P-Standard-Contract-Clauses-UK-Data-Transfers.pdf

“Non-European Data Protection Law” means data protection or privacy laws in force outside the EEA, Switzerland and the UK.

“Notification Email Address” means the email address(es) designated by Customer in the Order Form or Ordering Document (as applicable), to receive certain notifications from Actifio. Customer is responsible for ensuring that its Notification Email Address remains current and valid.

“Security Measures” has the meaning given in Section 7.1.1 (Actifio’s Security Measures).

“Subprocessor” means a third party authorized as another processor under these Data Processing and Security Terms to have logical access to and process Customer Data in order to provide parts of the Services and Technical Support Services (“TSS”).

“Supervisory Authority” means, as applicable: (a) a “supervisory authority” as defined in the EU GDPR; and/or (b) the “Commissioner” as defined in the UK GDPR.

“Term” means the period from the Full Activation Date until the end of Actifio’s provision of the Services under this Agreement, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Actifio may continue providing the Services for transitional purposes.

“UK GDPR” means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

2 The terms “personal data”, “data subject”, “processing”, “controller” and “processor” as used in these Data Processing and Security Terms have the meanings given in the GDPR, irrespective of whether European Data Protection Law or Non-European Data Protection Law applies.

3 Duration.

These Data Processing and Security Terms will, notwithstanding expiry or termination of the Term, remain in effect until, and automatically expire upon, deletion of all Customer Data by Actifio as described in these Data Processing and Security Terms.

4 Scope of Data Protection Law.

4.1 Application of European Law. The parties acknowledge that European Data Protection Law will apply to the processing of Customer Personal Data if, for example:

a. the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA or the UK; and/or

b. the Customer Personal Data is personal data relating to data subjects who are in the EEA or the UK and the processing relates to the offering to them of goods or services in the EEA or the UK, or the monitoring of their behaviour in the EEA or the UK.

4.2 Application of Non-European Law. The parties acknowledge that Non-European Data Protection Law may also apply to the processing of Customer Personal Data.

4.3 Application of Data Processing and Security Terms. Except to the extent these Terms states otherwise, these Terms will apply irrespective of whether European Data Protection Law or Non-European Data Protection Law applies to the processing of Customer Personal Data.

5 Processing of Customer Personal Data.

5.1 Roles and Regulatory Compliance; Authorization.

5.1.1. Processor and Controller Responsibilities. If European Data Protection Law applies to the processing of Customer Personal Data:

a. the subject matter and details of the processing are described in Appendix 1;

b. Actifio is a processor of that Customer Personal Data under European Data Protection Law;

c. Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Law; and

d. each party will comply with the obligations applicable to it under European Data Protection Law with respect to the processing of that Customer Personal Data.

5.1.2. Authorization by Third Party Controller. If European Data Protection Law applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants that its instructions and actions with respect to that Customer Personal Data, including its appointment of Actifio as another processor, have been authorized by the relevant controller.

5.1.3. Responsibilities under Non-European Law. If Non-European Data Protection Law applies to either party's processing of Customer Personal Data, the relevant party will comply with any obligations applicable to it under that law with respect to the processing of that Customer Personal Data.

5.2 Scope of Processing.

5.2.1 Customer's Instructions. Customer instructs Actifio to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and TSS; (b) as further specified via Customer's use of the Services and TSS; (c) as documented in the form of this Agreement, including these Data Processing and Security Terms; and (d) as further documented in any other written instructions given by Customer and acknowledged by Actifio as constituting instructions for purposes of these Data Processing and Security Terms.

5.2.2 Actifio's Compliance with Instructions. As from the Full Activation Date (at the latest), Actifio will comply with the instructions described in Section 5.2.1 (Customer's Instructions) (including with regard to data transfers) unless European or National Law to which Actifio is subject requires other processing of Customer Personal Data by Actifio, in which case Actifio will notify Customer (unless that law prohibits Actifio from doing so on important grounds of public interest) before such other processing.

6 Data Deletion

6.1 Deletion During Term. Actifio will enable Customer to delete Customer Data during the applicable Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the applicable Term and that Customer Data cannot be recovered by Customer, this use will constitute an instruction to Actifio to delete the relevant Customer Data from Actifio's systems in accordance with applicable law. Actifio will comply with this instruction as soon as reasonably practicable, unless European or National Law requires storage.

6.2 Deletion on Term Expiry. On expiry of the applicable Term, Customer instructs Actifio to delete all Customer Data (including existing copies) from Actifio's systems in accordance with applicable law. Actifio will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European or National Law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer is responsible for exporting, before the applicable Term expires, any Customer Data it wishes to retain.

7 Data Security.

7.1 Actifio's Security Measures, Controls and Assistance.

7.1.1 Actifio's Security Measures. Actifio will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, including measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Actifio's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness ("Security Measures"). Actifio may update these Security Measures from time to time provided that such updates do not result in the degradation of the overall security of the Services.

7.1.2 Security Compliance by Actifio Staff. Actifio will: (a) take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, and (b) ensure that all persons authorized to process Customer Personal Data are under an obligation of confidentiality.

7.1.3 Additional Security Controls. Actifio will make Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Data; and (b) provide Customer with information about securing, accessing and using Customer Data.

7.1.4 Actifio Security Assistance. Actifio will (taking into account the nature of the processing of Customer Personal Data and the information available to Actifio) assist Customer in ensuring compliance with its obligations pursuant to Articles 32 to 34 of the GDPR, by:

a. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Actifio's Security Measures);

b. making Additional Security Controls available to Customer in accordance with

Section 7.1.3 (Additional Security Controls);

c. complying with the terms of Section 7.2 (Data Incidents);

d. providing Customer with the information contained in these Data Processing and Security Terms.

7.2 Data Incidents

7.2.1 Incident Notification. Actifio will notify Customer promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2 Details of Data Incident. Actifio's notification of a Data Incident will describe, to the extent possible, the nature of the Data Incident, the measures taken to mitigate the potential risks and the measures Actifio recommends Customer take to address the Data Incident.

7.2.3 Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Actifio's discretion, by direct communication (for example, by phone call or an in-person meeting).

7.2.4 No Assessment of Customer Data by Actifio. Actifio has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

7.2.5 No Acknowledgement of Fault by Actifio. Actifio's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Actifio of any fault or liability with respect to the Data Incident.

7.3 Customer's Security Responsibilities and Assessment.

7.3.1 Customer's Security Responsibilities. Without prejudice to Actifio's obligations under Sections 7.1 (Actifio's Security Measures, Controls and Assistance) and 7.2 (Data Incidents), and elsewhere in the applicable Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Actifio's or Actifio's Subprocessors' systems, including:

a. using the Services and Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Data;

b. securing the account authentication credentials, systems and devices Customer uses to access the Services; and

c. retaining copies of its Customer Data as appropriate.

7.3.2 Customer's Security Assessment. Customer agrees, based on its current and intended use of the Services, that the Services, Security Measures, Additional Security

Controls and Actifio's commitments under this Section 7 (Data Security): (a) meet Customer's needs, including with respect to any security obligations of Customer under European Data Protection Law and/or Non-European Data Protection Law, as applicable, and (b) provide a level of security appropriate to the risk in respect of the Customer Data.

7.4 Reserved.

7.5 Reviews and Audits of Compliance.

7.5.1 If European Data Protection Law applies to the processing of Customer Personal Data, Actifio will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Actifio's compliance with its obligations under these Data Processing and Security Terms in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). Actifio will contribute to such audits as described in this Section 7.5 (Reviews and Audits of Compliance).

7.5.2. If Customer has entered into the Model Contract Clauses as described in Section 10.2 (Transfers of Data), Actifio will, allow Customer or an independent auditor appointed by Customer to conduct audits as described in the Model Contract Clauses in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

7.5.3 Additional Business Terms for Reviews and Audits.

a. Customer must send any requests for audits under Section 7.5.1 or 7.5.2 to Actifio's Data Protection Team as described in Section 12 (Data Protection Team; Processing Records).

b. Following receipt by Actifio of a request under Section 7.5.3(a, Actifio and Customer will discuss and agree in advance on the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit.

c. Actifio may charge a fee (based on Actifio's reasonable costs) for any audit. Actifio will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

d. Actifio may object in writing to an auditor appointed by Customer to conduct any audit if the auditor is, in Actifio's reasonable opinion, not suitably qualified or independent, a competitor of Actifio or Google, or otherwise manifestly unsuitable. Any such objection by Actifio will require Customer to appoint another auditor or conduct the audit itself.

7.5.4 No Modification of MCCs. Nothing in this Section 7.5 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or Actifio under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data).

8 Impact Assessments and Consultations. Actifio will (taking into account the nature of the processing and the information available to Actifio) assist Customer in ensuring compliance with its obligations pursuant to Articles 35 and 36 of the GDPR, by:

a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls)

b. providing the information contained in this Agreement and these Data Processing and Security Terms.

9 Access etc.; Data Subject Rights; Data Export

9.1 Access; Rectification; Restricted Processing; Portability. During the applicable Term, Actifio will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, and to export Customer Data.

9.2 Data Subject Requests.

9.2.1 Customer's Responsibility for Requests. During the applicable Term, if Actifio's Data Protection Team receives a request from a data subject in relation to Customer Personal Data, and the request identifies Customer, Actifio will advise the data subject to submit their request to Customer. Customer will be responsible for responding to any such request.

9.2.2 Data Subject Request Assistance. Actifio will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its obligations under Chapter III of the GDPR to respond to requests for exercising the data subject's rights by:

a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls);

b. complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Customer's Responsibility for Requests); and

c. if subsections (a) and (b) above are insufficient for Customer to comply with such obligations, upon Customer's request, providing additional reasonable assistance.

10 Data Transfers

10.1 Data Storage and Processing Facilities. Actifio may store and process Customer Data anywhere Actifio or its Subprocessors maintain facilities, subject to Section 10.2 (Transfers of Data) with respect to the Model Contract Clauses or Alternative Transfer Solution.

10.2 Transfers of Data. If the storage and/or processing of Customer Personal Data

involves transfers of Customer Personal Data from the EEA, Switzerland or the UK to any third country that does not ensure an adequate level of protection under European Data Protection Law ("Transferred Personal Data"), and European Data Protection Law applies to those transfers, then:

a. if Customer (as data exporter) enters into the Model Contract Clauses with Actifio (as data importer), then:

i. the transfers will be subject to the Model Contract Clauses

ii. The Model Contract Clauses (MCC EU Controller-to-Processor and/or MCC UK Controller-to-Processor, as applicable) are hereby agreed to between the Parties; and

ii. Actifio will ensure that Actifio complies with its obligations under the Model Contract Clauses in respect of those transfers; or

b. if Customer does not enter into the Model Contract Clauses as described in Section 10.2(a), then:

i. if an Alternative Transfer Solution is made available by Actifio: (A) Customer will be deemed to be using it and will take any action (which may include execution of documents) strictly required to give it full effect; and (B) Actifio will ensure that the transfers are made in accordance with such Alternative Transfer Solution; or

ii. if an Alternative Transfer Solution is not made available by Actifio: (A) Customer (as data exporter) will be deemed to have entered into the Model Contract Clauses with Actifio (as data importer); (B) the transfers will be subject to the Model Contract Clauses; and (C) Actifio will ensure Actifio complies with its obligations under the Model Contract Clauses in respect of those transfers; and

c. if Customer has entered into the Model Contract Clauses but reasonably determines subsequently that they do not provide an adequate level of protection, then:

i. if an Alternative Transfer Solution is made available by Actifio, Customer may, by notifying Actifio via Actifio's Data Protection Team in accordance with Section 12.1, terminate any Model Contract Clauses applicable under Section 10.1(a), such that Section 10.2(b)(i) will apply; or

ii. if an Alternative Transfer Solution is not made available by Actifio, Customer may terminate the Agreement immediately by notifying Actifio.

10.3 Data Center Information. Our Service is currently hosted in data centers provided by Google Cloud. Information about the locations of Google facilities is available at: https://cloud.google.com/about/locations/ (as may be updated by Google from time to

time).

10.4 Disclosure of Confidential Information Containing Personal Data. If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data), Actifio will, notwithstanding any term to the contrary in the applicable Agreement, ensure that any disclosure of Customer's Confidential Information containing personal data, and any notifications relating to any such disclosures, will be made in accordance with such Model Contract Clauses.

11 Subprocessors

11.1 Consent to Subprocessor Engagement. Customer specifically authorizes the engagement as Subprocessors of: (a) those entities listed as of the Full Activation Date at the URL specified in Section 11.2 (Information about Subprocessors); and (b) all other Google Affiliates from time to time. In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessor Changes), Customer generally authorizes the engagement as Subprocessors of any other third parties ("Third Party Subprocessors"). If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data), the above authorizations constitute Customer's prior written consent to the subcontracting by Actifio of the processing of Customer Data.

11.2 Information about Subprocessors. Actifio utilizes Google Cloud for the Services as the cloud hosting provider. More information is available about Google Cloud's downstream subprocessors, including their functions and locations, at https://cloud.google.com/terms/subprocessors. In addition, Actifio may also utilize Persistent Systems Limited to support the provision of the TSS.

11.3 Requirements for Subprocessor Engagement. When engaging any Subprocessor, Actifio will:

a. ensure via a written contract that:

i. the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this Data Processing and Security Terms) and any Model Contract Clauses entered into or Alternative Transfer Solution adopted by Actifio as described in Section 10.2 (Transfers of Data); and

ii. if the GDPR applies to the processing of Customer Personal Data, the data protection obligations described in Article 28(3) of the GDPR, as described in these Data Processing and Security Terms, are imposed on the Subprocessor; and

b. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4 Opportunity to Object to Subprocessor Changes.

a. When any new Third Party Subprocessor is engaged during the applicable Term, Actifio will notify Customer of the engagement.

b. Customer may, within 30 days after being notified of the engagement of a new Third Party Subprocessor, object by terminating the applicable Agreement immediately upon written notice to Actifio. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

12 Data Protection Team; Processing Records

12.1 Actifio's Data Protection Team. Actifio's Data Protection Team can be contacted by sending an email to support@actifio.com and/or by Customer by providing a notice to Actifio as described in this Agreement.

12.2. Actifio's Processing Records. To the extent the GDPR requires Actifio to collect and maintain records of certain information relating to Customer, Customer will, where requested, utilize the Services to supply such information and keep it accurate and up-to-date. Actifio may make any such information available to the Supervisory Authorities if required by the GDPR.

13 Liability

13.1 Liability Cap. If Model Contract Clauses have been entered into as described in Section 10.2 (Transfers of Data) then, subject to Section 13.2 (Liability Cap Exclusions), the total combined liability of either party and its Affiliates towards the other party and its Affiliates under or in connection with the applicable Agreement and such Model Contract Clauses combined will be limited to the Agreed Liability Cap for the relevant party.

13.2 Liability Cap Exclusions. Nothing in Section 13.1 (Liability Cap) will affect the remaining terms of this Agreement relating to liability (including any specific exclusions from any limitation of liability).

14 Third Party Beneficiary

Notwithstanding anything to the contrary in this Agreement, where Google LLC is not a party to such Agreement, Google LLC will be a third party beneficiary of Sections 7.5 (Reviews and Audits of Compliance), 11.1 (Consent to Subprocessor Engagement) and 13 (Liability).

15 Conflict of Terms

Notwithstanding anything to the contrary in this Agreement, to the extent of any conflict or inconsistency between the terms of these Data Processing and Security Terms and the remainder of this Agreement, these Data Processing and Security Terms will govern.

v.22.03