APPENDIX 2

DATA PROCESSING AGREEMENT

1. PURPOSE

This Data Processing Agreement ("**DPA**") regulates the parties' rights and obligations in connection with Ardoq ("**Data Processor**") processing personal data on behalf of the Customer ("**Data Controller**"). The purpose of the DPA is to comply with the requirements for data processor agreements according to Data Protection Laws. "**Data Protection Laws**" mean any laws applicable to the processing of Personal Data under the Agreement, including but not limited to, the General Data Protection Regulation EU 2016/679 and the United Kingdom Data Protection Act 2018 (including UK GDPR) (jointly "**GDPR**"). Personal Data, Processing, Subprocessors, Breach, Data Controller and Data Processor shall have the meanings given to them under Data Protection Laws. The Term "Personal Data" includes "Personal Information" and "Personally Identifiable Information"; "Data Processor" includes "Service Provider"; "Data Subject" includes "Principal" or "Consumer".

2. SCOPE OF PROCESSING

2.1 Personal Data. The Data Processor will Process the following types of Personal Data on behalf of the Data Controller:

- Name, business email address, IP address, title,
- other Personal Data inserted into the Service by Data Controller.

2.2 Data Subjects. The Personal Data is connected to the following categories of Data Subjects:

- Users.
- Other Data Subjects whose Personal Data are uploaded into the Service by Data Controller.

2.3 Purpose. The Data Processor shall process the Personal Data for the following purposes:

- Fulfilling the Agreement with the Data Controller.

2.4 Duration of processing

- Duration of the Agreement.

2.5 Subject-matter and nature of processing

- Provision of the Services, as defined in the Agreement.

3. DATA PROCESSOR'S DUTIES

3.1 Compliance with Instructions. When Processing Personal Data on behalf of the Data Controller, the Data Processor shall follow Data Controller's instructions, unless otherwise provided by applicable laws. The parties agree that this DPA represents the original instructions of the Data Controller. Data Controller may submit new instructions in writing, provided that such new instructions will be consistent with the scope and purpose of the Services purchased. Data Processor shall use reasonable effort to promptly notify Data Controller if it believes that new instructions might be violating Data Protection Laws, provided however that Data Controller remains solely responsible for the lawful collection and upload of Personal Data into the Services.

3.2 Confidentiality. The Data Processor is subject to an obligation of confidentiality regarding data that the Data Processor gets access to under the DPA. This provision also applies after the termination of the DPA. The Data Processor is obliged to ensure that persons who process the Personal Data for the Data Processor have committed themselves to confidentiality.

3.3 General Duty of Cooperation. Data Processor shall assist the Data Controller in ensuring compliance with its obligations under Data Protection Laws. Data Controller acknowledges and agrees that, taking into account the automated nature of the Processing performed by the Data Processor and that the Services are of a self-service nature, where all data input are administered directly by Data Controller, this assistance might be provided by making available to the Data Controller automated means to manage and administer Personal Data in the Services.

4. SUB-PROCESSORS

4.1 General Consent. Data Controller consents to the use by Data Processor of the Subprocessors listed as https://www.ardoq.com/sub-processors as of the Effective Date of this Agreement.

4.2. New Subprocessors. In addition, the Data Processor has the right to add or replace Subprocessors, but is obliged to inform the Data Controller of any such intended changes, so that the Data Controller has the opportunity to object to the changes. The information shall be given at least 30 calendar days prior to the planned changes taking effect. In order to receive such notification, Data Controller shall register at https://www.ardoq.com/sub-processors. The Data Controller has a right to object to the change in writing within the above period, explaining reasonable grounds for objections, and the parties shall use reasonable efforts to solve the objection of Data Controller. If the parties cannot find an agreement and Data Processor decides to proceed with the change despite the Data Controller's reasonable objections, the Data Controller has the right to terminate the Agreement no later than 30 calendar days after the change is implemented.

4.3. Obligations of Data Processor respect to Subprocessors. Data Processor shall ensure that its agreements with the Subprocessors include obligations consistent with those set forth in this DPA. The Data Processor shall remain fully liable to the Data Controller for the acts and omissions of any Subprocessors under the Agreement as if they were its own.

5. TRANSFERS OF PERSONAL DATA SUBJECT TO GDPR

To the extent Processing under the Agreement is subject to the GDPR, the Data Processor commits to not transfer the Personal Data processed on behalf of Data Controller hereunder outside the EEA (including the EU), UK and Switzerland, unless it has ensured that there is a legal basis for the transfer of such Personal Data outside the GDPR Area or unless required by mandatory provisions of applicable law.

6. SECURITY AND BREACHES

6.1 ISMS. The Data Processor shall through planned and systematic measures implement appropriate technical and organizational measures to ensure a satisfactory level of security, e.g. in

relation to confidentiality, integrity and availability. The Information Security Management System applicable as of the effective date of the Agreement is described in Appendix 3.

6.2 Notification of Breaches. The Data Processor shall notify the Data Controller without undue delay - and in any case no later than 72 hours - after becoming aware of a Breach impacting the Data Controller's Personal Data. The notification shall contain sufficient information so that the Data Controller may assess whether the Breach must be notified to the authorities or to the Data Subjects. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

6.3 Notification contact details. Breach notifications will be made via email to the security contact(s) provided by Data Controller in the Services. Data Controller acknowledges that it is responsible for maintaining up to date contacts during the course of the Term. Multiple contacts are possible.

6.4 Notifications to Authorities and Data Subjects. Unless otherwise required by Data Protection Laws, Data Controller shall determine for any Breach (i) whether and when notice will be provided to any authority and which authority to notify; (ii) whether and when notice will be provided to Data Subjects; (iii) the content of any such notice(s); (iv) the timing for, and method of, delivery of any such notice(s). The Data Processor shall provide reasonable cooperation to such notification efforts, however the Data Processor shall neither be obligated nor authorized to make any such notifications on behalf of the Data Controller.

7. DOCUMENTATION AND SECURITY AUDITS

7.1 Security Documentation and reports. The Data Processor shall maintain reasonable documentation that proves that the Data Processor complies with its obligations under this DPA and regularly conduct security audits as required to maintain ISO27001 and SOC2 Type 2 certifications. Data Processor shall make such documentation, including certifications and with the results of such audits, available to the Data Controller upon request.

7.2 Audits. To the extent the documentation and the audit reports are not sufficient to address the Data Controller's reasonable audit requirements under Data Protection Laws, Data Controller may request additional information in writing or conduct audits and inspections ("**Audit**"). Data Controller shall use reasonable efforts to limit its Audit requests to one per calendar year, unless in case of Breach, and shall cooperate with Data Processor to avoid disruptions to Data Processor's business operations, including by jointly agreeing on the agenda of the Audit. The above audits may be carried out by the Data Controller or a third party mandated by the Data Controller in agreement with the Data Processor. To the extent the Data Controller requires additional assistance from the Data Processor, the Data Processor may offer such assistance as a separately paid service.

7.3 Outcome of an Audit. The outcome of an Audit shall be considered Confidential Information of Data Processor. Data Processor shall promptly address at its own costs any non compliance identified by the Audit.

8. DATA SUBJECTS RIGHT REQUESTS

8.1 Automated Means. Data Processor shall make available to Data Controller automated technical and organisational measures for the fulfilment of Data Controller's obligation to respond to requests of Data Subjects for exercising their rights under Data Protection Laws in regard to the Personal Data processed in the Services on behalf of the Data Controller. To the extent the Data Controller requires additional assistance from the Data Processor, the Data Processor may offer such assistance as a separately paid service.

8.2 DSR. Should the Data Processor receive a data subject request directly from a Data Subject concerning the exercise of their rights with respect to the Personal Data processed pursuant to this DPA, the Data Processor shall not answer it directly unless to the extent mandatorily required by Data Protection Laws, and it shall promptly instruct said Data Subject to contact the Data Controller instead.

9. ASSISTANCE TO CARRY OUT DPIA

Whenever a data protection impact assessment (DPIA) is required, the Data Processor shall assist the Data Controller in carrying out such DPIA and relevant prior consultations (including - to the extent applicable - pursuant to GDPR Articles 35 to 36), taking into account the nature of the processing and the information available to the Data Processor.

10. TERM OF THE DPA

The DPA applies as long as the Data Processor processes Personal Data on behalf of the Data Controller in connection with providing the Service to the Data Controller.

11. TERMINATION

The DPA may only be terminated together with the Agreement, in accordance with the termination clauses in the subscription terms. Termination of the subscription terms also constitutes a termination of the DPA.

12. RETURN AND/OR DELETION OF DATA UPON TERMINATION OF THE DPA

12.1 Return. The Data Processor shall make available to the Data Controller a standard feature allowing the Data Controller to export the Personal Data from the Services at any time during the Term. Following the expiration or termination of the Term, Data Processor shall support Data Controller in retrieving Personal Data upon request, provided that such request is provided at least 10 days prior to the expiration of the Retention Period.

12.2 Deletion. Except to the extent prohibited to do so by law, the Data Processor will permanently erase all Personal Data processed as part of Customer Data on behalf of the Data Controller following the lapse of a standard 90 calendar days retention period from termination or expiration of the Agreement ("**Retention Period**").