Harbor Data Processing Agreement (online)

1. The customer agreeing to these terms ("**Customer**"), and **Revevol Italia,** having its principal place of business at Via Carducci 125-A, 20099 Sesto San Giovanni **(Supplier**), have entered into an agreement under which Supplier has agreed to provide certain Services, which may be amended from time to time (the "Agreement").

2. This Data Processing Agreement and its appendices (the "**DPA**"), which is between Supplier and Customer (each, a "**Party**", and together, "**the Parties**"), forms part of the Agreement and is the Parties' agreement related to Supplier's processing of Customer's Data. This DPA might be updated from time to time and will be effective and replace any previously applicable data processing agreement as from the Terms Effective Date (as defined below). To the extent of any conflict or inconsistency between the terms of this DPA and the remainder of the Agreement, the terms of this DPA will govern. Definitions are provided in Section 26.

3. The Parties acknowledge and agree that (a) under the Data Protection Legislation, Supplier is a Data Processor of Customer Personal Data listed in **Appendix 1**, (b) Customer subscribing to Supplier's services may be a Data Controller or Data Processor, as applicable, of Customer Personal Data and (c) each Party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the Processing of that Customer Personal Data.

4. Details on categories of data processed and data subjects concerned, processing operations, location of processing, and purpose and duration of processing are provided in **Appendix 1**.

5. **Duration.** This DPA will take effect on the Agreement Effective Date and, notwithstanding expiry of the Term, remains in effect until, and automatically expire upon, deletion of all Customer Data by Supplier as described in this DPA.

6. **Scope.** The Parties acknowledge and agree that the Data Protection Legislation will apply to the Processing of Customer Personal Data if: (a) the Processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA/Switzerland; and/or (b) the Customer Personal Data relates to Data Subjects who are in the EEA/ Switzerland and the Processing relates to the offering of goods or services in the EEA or the monitoring of their behaviour in the EEA.

7. **Non-European Data Protection Legislation**. The Parties acknowledge and agree that Non-European Data Protection Legislation may also apply to the Processing of Customer Personal Data. Except to the extent this DPA states otherwise, the terms of this DPA will apply irrespective of whether the Data Protection Legislation or Non-European Data Protection Legislation applies to the Processing of Customer Personal Data by Supplier. If Non-European Data Protection Legislation applies to either Party's Processing of Customer Personal Data, the Parties acknowledge and agree that the relevant Party will comply with any obligations applicable to it under that legislation with respect to the Processing of that Customer Personal Data.

8. **Third-party Data Controller.** If the Data Protection Legislation applies to the Processing of Customer Personal Data and Customer is a Data Processor acting under the instructions of a third-party Data Controller, Customer warrants to Supplier that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment as Data Processor have been authorized by the Third Party Data Controller and shall provide evidence thereof, at Supplier's request.

9. **Customer's Instructions**. By entering into this DPA, Customer instructs Supplier to Process Customer Personal Data only in accordance with the Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable: (a) to provide the Services and related technical support; (b) as further specified by Customer or required by Customer's use of the Services and related technical support; (c) as documented in the form of the Agreement, including this DPA; and (d) as further documented in any other legitimate and written instructions given by Customer and acknowledged by Supplier as constituting instructions for purposes of this DPA. As from the Effective Date, Supplier will comply with the Customer's instructions provided in this Section, including with regard to Personal Data transfers, in accordance with Section 21. Supplier shall not process, transfer, modify, amend or alter Customer Personal Data or disclose or permit the disclosure of the Customer Personal Data to any third-party other than in accordance with the Customer's instructions (whether in the Agreement or otherwise) unless EU law or EU Member State law to which Processor is subject requires other Processing of Customer Personal Data by Supplier, in which case Supplier will inform Customer prior to implement the processing (unless that law prohibits Processor from doing so on important grounds of public interest) via the Notification Email Address. Supplier agrees to immediately inform the Customer if, in its opinion, an instruction infringes the applicable Data Protection Legislation.

10. **Deletion During Term.** Supplier will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer or an End User uses the Services to delete any Customer Data during the Term and the Customer Data cannot be recovered by Customer or an End User, this use will constitute a Customer's Instruction to Supplier to delete the relevant Customer Data from Supplier's Systems in accordance with applicable Data Protection Legislation. Supplier will comply with this instruction as soon as reasonably practicable and within a maximum period of 90 days, unless EU or EU Member State law requires or justifies that such Personal Data be retained by Supplier for a longer period of time.

11. **Deletion on Term Expiry.** Subject to Section 12 (Deferred Deletion Instructions), upon expiry of the Term, Customer instructs Supplier to delete all Customer Data (including existing copies) from Supplier's Systems in accordance with applicable Data Protection Law. Processor will comply with this Instruction as soon as reasonably practicable and within a maximum period of 90 days, unless EU or EU Member State law requires or justifies that such Personal Data be retained by Processor for a longer period of time. Without prejudice to Section 20 (Data Subjects Rights and Requests) Customer acknowledges and agrees that Customer will be responsible for exporting, before the Term expires, any Customer Data it wishes to retain afterwards.

12. **Deferred Deletion Instruction.** To the extent any Customer Data covered by the deletion instruction described in Section 11 (Deletion on Term Expiry) is also processed, when the Term under Section 11 expires, in relation to an agreement between Customer and Supplier having a continuing Term, such deletion instruction will only take effect with respect to such Customer Data when the continuing Term expires. For clarity, in the event of a Deferred Deletion Instruction, this DPA will continue to apply to such Customer Data until its deletion by Supplier.

13. **Supplier Security Measure.** Supplier will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "**Security Measures**"). As described in **Appendix 2**, the Security Measures include measures to help ensure ongoing confidentiality, integrity, availability and resilience of Supplier's Systems, restore timely access to Customer Data following a Data Incident and

regular testing of effectiveness. Supplier may update or modify the Security Measures in **Appendix 2** from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services or Supplier's Systems. Customer acknowledges that Customer Data will be hosted in a **Third-Party Service Provider** data centres, by **Third-Party Service Provider** and/or one or more of its affiliated entities (collectively, "**Third-Party Service Providers"**) (and not by the Supplier) and, as a consequence, that most of the technical and organisational security measures relating to the Customer Data (as notably referred to in **Appendix 2**) will be provided by the applicable **Third-Party Service Provider** under its own liability. Accordingly, and notwithstanding any other provision in the Agreement, the Supplier disclaims any and all responsibility in relation to any acts and/or omission of **Third-Party Service Provider**, including notably (without limitation) for such **Third-Party Service Provider's** technical and organisational security measures as listed for information purposes only and without any representation in Appendix 2. Customer agrees to disclaim Supplier's liability, in the event of any non-compliance of the **Third-Party Service Provider** under the applicable agreement.

14. **Security Compliance by Processor**. Supplier will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors, agents and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that such personnel has undertaken appropriate training in accordance with the Data Protection Legislation.

15. **Processor Security Assistance.** Customer agrees that Supplier will (taking into account the nature of the Processing of Customer Personal Data and the information available to Supplier) assist Customer in ensuring compliance with Customer's obligations in respect of security of Personal Data and Personal Data breaches, in particular in the event of a Data Incident, including if applicable Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by: (a) implementing and maintaining the Security Measures in accordance with Section 13 (Supplier's Security Measures); (b) complying with the terms of Section 16 (Data Incidents).

16. **Data Incidents.** If Supplier becomes aware of a Data Incident, Supplier will: (a) notify Customer of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimize harm and secure Customer Data. Notifications will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Supplier recommends Customer to take to address the Data Incident. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Supplier's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid at any time. Supplier will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with notification obligations provided by Data Protection Legislation or Non-European Data Protection Legislation, as applicable to Customer, and fulfilling any third party notification obligations related to any Data Incident(s). Supplier's notification of or response to a Data Incident under this Section 16 (Data Incidents) will not be construed as an acknowledgement by Supplier of any fault or liability with respect to the Data Incident.

17. **Customer's Security Responsibilities and Assessment**. Customer agrees that, without prejudice to Supplier's obligations under Sections 13-15 (Supplier's Security Measures, Controls and Assistance) and Section 16 (Data Incidents): (a) Customer is solely responsible for its use of the Services, including: (i)

making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Data; (ii) securing the account authentication credentials, systems and devices Customer uses to access the Services; and (iii) backing up Customer Data; and (b) Supplier has no obligation to protect Customer Data that Customer elects to store or transfer outside of Processor's and its Subprocessors' systems (for example, offline or on-premise storage, or Customer's Third-Party Service Provider). Customer is solely responsible for evaluating whether the Services, the Security Measures and Supplier's commitments under Sections 13-17 meet Customer's needs, including with respect to any security obligations of Customer under the Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Supplier as set out in Section 13 (Supplier's Security Measures) and **Appendix 2** provide a level of security appropriate to the risk in respect of the Customer Data.

18. **Audits of compliance**. If the Data Protection Legislation applies to the Processing of Customer Personal Data, Supplier will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Supplier's compliance with its obligations under this DPA. Supplier will contribute to such audits as described in this Section 18 (Audits of Compliance). If Customer decides to conduct an audit as described above, then Customer shall bear all costs and expenses connected therewith, such as the auditors' fees, costs of transport, legal fees, etc. If Customer has entered into Model Contract Clauses as described in Section 21 (Personal Data Transfer),Supplier will, without prejudice to any audit rights of a Supervisory Authority under such Model Contract Clauses, allow Customer or an independent auditor appointed by Customer to conduct audits as described in the Model Contract Clauses. Customer may also conduct an audit to verify Supplier's compliance with its obligations under this DPA. In any event, any audit mandated by Customer pursuant to this Section 18 shall not impair or otherwise trouble Supplier's usual course of business.

19. **Impact Assessments and Consultations**. Customer agrees that Supplier will (taking into account the nature of the Processing and the information available to Processor) provide Customer with reasonable assistance in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR, to the extent necessary information is available to Supplier.

20. **Data Subject Rights and Request**. During the Term, Supplier will, in a manner consistent with the functionality of the Services, enable Customer to access, rectify and restrict Processing of Customer Data, or erase Customer Data, as applicable, including via the deletion functionality provided by Supplier as described in Section 10 (Deletion During Term), and to export Customer Data, as required by Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable. During the Term, if Supplier receives any request from a Data Subject in relation to Customer Personal Data, Supplier will advise the Data Subject to submit his/her request to Customer or directly report such request to Customer using the Notification Email Address or any other communication channel, and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services. Customer agrees that (taking into account the nature of the Processing of Customer Personal Data) Supplier will provide Customer with reasonable assistance in fulfilling any obligation to respond to requests by Data Subjects, including if applicable Customer's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR, by complying with the commitments set out in this Section 20, to the extent Supplier is able to respond to such requests.

21. **Personal Data Transfer**. Customer acknowledges and agrees that Supplier may, subject to this Section 21 (Personal Data Transfer), store and process Customer Data in the United States and any other country outside the EEA in which Supplier or Subprocessors maintain facilities. If the storage and/or Processing of Customer Personal Data involves a Restricted Transfer, Supplier and Customer hereby agree to enter into the Model Contract Clauses enclosed in **Appendix 4**. In such case, any Restricted Transfers are made in accordance with such Model Contract Clauses. Supplier will impose under a written agreement the same obligations on the Subprocessors, if any, as are imposed on the Processor under this DPA and the Model Contract Clauses. Where the Subprocessor fails to fulfil its data protection obligations under such written agreement, the Supplier shall remain fully liable to the Customer for the performance of the Subprocessor's obligations under such agreement. In addition, where provision of the Services involves a Restricted Transfer from the Supplier to a Subprocessor located outside EU, Customer (on behalf of itself and its relevant Affiliates) mandates Supplier, which mandate Supplier hereby accepts, to promptly enter, on Customer's own name and behalf as Data Exporter (Subprocessor being the Data Importer), into a Personal Data processing agreement with any Subprocessor engaged by Supplier in such Restricted Transfer, before such Subprocessor first Processes the Personal Data, so as to ensure that any such Restricted Transfer complies with the Data Protection Legislation. Such Personal Data processing agreement shall (a) meet the conditions set out in Article 28 of the GDPR and offer at least the same level of protection for the Personal Data as those set out in this DPA and (b) incorporate Model Contract Clauses. When Supplier uses Third Party Service Provider Cloud Platform to host and/or provide the Services, information about the locations of Supplier's Third Party Service Providers' data centers is available at the Third Party Service Providers' pages specifying servers locations and may be updated by the Third Party Service Provider from time to time. If Customer has entered into Model Contract Clauses as described in this Section 21 (Personal Data Transfer), Supplier will, notwithstanding any term to the contrary in the Agreement, ensure that any disclosure of Customer's Confidential Information containing Customer Personal Data, and any notifications relating to any such disclosures, will be made in accordance with such Model Contract Clauses.

22. **Subprocessors**. Customer hereby specifically authorizes the engagement of Supplier's Affiliates as Subprocessors pursuant to the Agreement and for the Term. In addition, Customer hereby generally authorizes the engagement of any other third parties as Subprocessors ("**Third Party Service Provider Subprocessors**"), subject to Supplier's compliance with this Section 22. Customer hereby authorizes all "Subprocessors" listed in **Appendix 3**. If Customer has entered into Model Contract Clauses as described in Section 21 (Personal Data Transfer), the above authorizations will constitute Customer's prior written consent to the subcontracting by Supplier of the Processing of Customer Data if such consent is required under the Model Contract Clauses and Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable. Information about Subprocessors is available in Appendix 3 and may be updated by Supplier from time to time in accordance with this DPA. When engaging any Subprocessor, Supplier will: (a) ensure via a written legal instrument or contract that: (i) the Subprocessor only accesses and processes Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this DPA) and any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data Out of the EEA), as applicable; and (ii) if the GDPR applies to the Processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this DPA, are mandated by said legal instrument or contract on the Subprocessor; and (b) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor. When any Third-Party Subprocessor not listed in Appendix 3 at the Agreement Effective Date is engaged during the Term, Supplier will, at least 30 days before the new Third-Party Subprocessor processes any Customer Data, inform Customer of the engagement (including the name and location of the

relevant Third-Party Subprocessor and the activities it will perform) by sending an email to the Notification Email Address. Customer may object to any new Third-Party Subprocessor by terminating the Agreement immediately upon written notice to Supplier, provided that Customer sends such notice within 90 days of being informed of the engagement of the Third-Party Subprocessor. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third-Party Subprocessor.

23. **Processing Records.** Customer acknowledges that Supplier is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of any Data Processor and/or Data Controller on behalf of which Processor is acting and, where applicable, of such Data Processor's or Data Controller's local representative and data protection officer, as well as the categories of Processing carried out on behalf of each Data Controller, where possible a general description of the technical and organisational security measures; and (b) make such information available to the Supervisory Authorities.

24. **Agreed Liability Cap**. The cap of liability set forth in the Agreement governing the provision of Services to which this DPA is part applies to any violation of the provisions of this DPA or any damage which may result from the Supplier's or its Affiliate's non-compliance with Data Protection Laws. Nothing in this Section 24 (Agreed Liability Cap) will affect the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability).

25. **Miscellaneous**.

25.1. Neither the rights nor the obligations of any Party may be assigned in whole or in part without the prior written consent of the other Party, provided, however, that this DPA may be transferred or assigned in the event of a restructuring or change of control affecting a Party hereto.

25.2. In the event of any dispute arising between the Parties in connection with this DPA, the Parties shall negotiate in good faith to resolve their dispute. If the dispute cannot be resolved by good faith negotiations by the Parties, the dispute shall be finally settled by a public court relevant for the seat of the Supplier.

25.3. This DPA is governed by the laws of France, without reference to its rules governing conflicts of laws.

25.4. Should any provision of this DPA be deemed invalid or unenforceable by a competent court, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

25.5. Any amendments to this Data Processing Agreement shall be made in writing, otherwise being null and void.

26. **Definitions.** Capitalized terms used but not defined in this DPA have the meanings given in the Agreement. In this DPA, unless stated otherwise:

"**Affiliate**" means any entity controlling, controlled by, or under common control with a Party, where "control" is defined as: (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

"**Agreement**" means the Services Agreement entered into between the Supplier and the Customer for the provision of Services by the Supplier to Customer.

"**Agreed Liability Cap**" means the maximum monetary or payment-based amount at which a Party's liability is capped under the Agreement, either per annual period or event giving rise to liability, as applicable.

"**Customer Data**" means data submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users. Customer Data may also include Personal Data sent or otherwise made available by Customer to Supplier and/or Supplier's Affiliates where Customer uses Supplier Affiliates Solutions. For the avoidance of doubt, for the purpose of the Agreement and the DPA, Customer Data does not include data contained in files stored in Customer's Third Party Service Provider Solution account(s) to which Supplier does not have access.

"**Customer Personal Data**" means Personal Data contained within the Customer Data, as described in Appendix 1.

"**Data Incident**" means a breach of Supplier's security measures 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 Supplier. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Effective Date**" means the date on which Customer and Supplier agreed to this DPA, and is the Agreement Effective Date.

"**EEA**" means the European Economic Area.

"**End User**" means natural persons authorized by Customer to access or use the Services, including Customer and Customer's Affiliate personnel, employee, agent or contractor.

"**Data Protection Legislation**" means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland) as well as any data protection laws substantially amending, replacing or superseding the GDPR, the Federal Data Protection Act of Switzerland and/or other applicable European Union Member state domestic data protection or national/federal or state/provincial privacy legislation in force, including where applicable, statutes, decisions, guidelines, guidance notes, codes of practice, codes of conduct and data protection certification mechanisms issued from time to time by competent court or Supervisory Authority, relating to the Processing of personal data and privacy.

"**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.

"**Model Contract Clauses**" or "MCCs" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as approved by the European Commission in Decision 2010/87/EU, as amended, replaced or superseded by any set of clauses approved by the European Commission. The Model Contract Clauses are enclosed as **Appendix 4** and are part of this agreement when applicable.

"**Non-European Data Protection Legislation**" means any national/federal or state/provincial/emirate data protection or privacy legislation, other than the Data Protection Legislation.

"**Notification Email Address(es)**" means the email address(es) designated by Customer to receive certain notifications from Supplier.

"**Supplier's Systems"** means the computing and storage infrastructure contracted by Supplier to run the Services and to store the Customer Data. For the avoidance of doubt, Supplier's Systems do not include Third-Party Service Provider Solution used by Customer and contracted by Customer, nor any of the Third Party Offerings.

"**Restricted Transfer**" means (a) a transfer of the Personal Data from Customer to Supplier or Subprocessor, or (b) an onward transfer of the Personal Data from Supplier or Subprocessor to (or between

two establishments of) Supplier or Subprocessor, in each case, being a transfer to a country outside the EEA, where such transfer would be prohibited by European Data Protection Legislation in the absence of Model Contract Clauses or other legal instruments required by European Data Protection Legislation.

"**Subprocessor(s)**" mean third parties authorized by Processor under this DPA to have logical access to and process Customer Data on behalf of Customer in order to provide parts of the Services and related technical support, including Supplier's Affiliates.

"**Security Measures**" has the meaning given in Section 13 (Supplier Security Measures).

"**Services**" means the services that have been purchased by the Customer pursuant to the Agreement and any applicable Order Form, including Harbor and any update or replacement thereof and technical support provided by Supplier to Customer from time to time. The Services do not include (i) Supplier Affiliates Solution that may have been separately licensed by Customer, (ii) any Third Party Offerings that may have been separately licensed by Customer, nor (iii) the Third-Party Service Provider Solution used by Customer.

"**Supplier Affiliates Solution**" means any solution of software provided by one or more Supplier's Affiliates, which supplements and/or are necessary to provide the Services performed by Supplier, that have either been (i) licensed by Customer from a Supplier's Affiliate or (ii) licensed by Customer from Supplier.

The terms "Personal Data", "Data Subject", "Processing", "Data Controller", "Data Processor" and "Supervisory Authority" as used in this DPA have the meanings given to them in the GDPR, and the terms "Data Importer" and "Data Exporter" have the meanings given to them in the Model Contract Clauses, in each case irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation applies.

"**Term**" means the period from the Agreement Effective Date until the end of Supplier's provision of the Services to Customer under the Agreement, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Supplier may continue providing the Services to Customer for transitional purposes.

"**Third-Party Service Provider Solution**" means any solution or software on which all or part of the Services are performed by the Supplier, that have been separately licensed by Customer, as the case may be, from an unaffiliated Third-Party Service Provider. Third Party Service Providers Solutions may notably include Google, Microsoft and/or Facebook solutions or software.

"Terms Effective Date" means the date on which Customer accepted, or the parties otherwise agreed to, these Terms.

Appendix 1 - Data Processing Details

Subject Matter	Supplier's provision of the Services and related technical support to Customer.
Categories of Data Subjects Categories of Data Subjects whose Personal Data will be Processed by Service Provider	Personal Data submitted, stored, sent or received via the Services may concern the following categories of Data Subjects: End Users including Customer's employees and contractors; the personnel of Customer's own customers, suppliers and subcontractors; and any other person who transmits data via the Services, including individuals collaborating and communicating with End Users.
Categories of data Personal Data that will be Processed by Supplier	Personal Data that will be Processed by Supplier includes data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services, including End Users' IDs and email addresses, Workplace posts, chats and comments.
Location of Processing Operations Locations where the personal data will be Processed by Supplier	Personal Data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services may be processed at Supplier's locations situated at: - 6 rue Beaubourg, 75004 Paris, France - 650 California Street, San Francisco, CA 94108, USA - 3280 Peachtree Road NE, 7th Floor Atlanta, GA 30305, USA - Via Giosue' Carducci 125/A, 20099 Sesto San Giovanni, Milan, Italy
Purposes Purposes for which the Personal Data will be Processed by Supplier	Supplier will process Customer Personal Data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services for the purposes of providing the Services and related technical support to Customer in accordance with the Data Processing Agreement.
Duration of processing The length of time for which Processing activities will be carried out Supplier	The applicable Term plus the period from expiry of such Term until deletion of all Customer Data by Supplier in accordance with the Data Processing Agreement.

Appendix 2 - Security Measures

1. As from the Agreement Effective Date, Supplier will implement and maintain the Security Measures set out in this Appendix 2 to the Data Processing Agreement. Supplier may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Supplier's System and of the Services.

2. **Infrastructure security**. Supplier uses G Suite and Google Cloud Platform (GCP) to host the Supplier's Systems. All of the Supplier's Systems are fully managed by Google Inc. (Google), who is responsible for the physical and networking security of the Supplier's Systems. Google's security measures regarding the G Suite and GCP infrastructures are described on this page (G Suite) https://gsuite.google.com/security/?secure-by-design_activeEl=data-centers and this page (Google Cloud Platform): https://cloud.google.com/security/

3. **Personnel Security**: Supplier personnel accessing Supplier's Systems are authenticated via their G Suite account, protected by the same physical, networking and organizational measures as described above. Supplier personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Supplier conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labour law and statutory regulations. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Supplier's confidentiality and privacy policies. Personnel are also required to undertake appropriate training on privacy and data protection principles in compliance with the Data Protection Legislation.

4. **Subprocessor Security.** Before onboarding Subprocessors, Supplier conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Supplier has assessed the risks presented by the Subprocessor, then subject always to the requirements set out in Section 22 (Requirements for Subprocessor Engagement) of this Data Processing Agreement, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Appendix 3 - Subprocessors

Supplier uses the following Subprocessors for the performance of the Services:

Entity name	**Corporate location**
Google Inc	USA

Appendix 4 - Model Contract Clauses

Model Contractual Clauses (processor) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Supplier (the "**Data Importer**") and Customer (the "**Data Exporter**"), each a "**party**", together "**the parties**", agree on the following Model Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in the Clauses Schedule 1. The Clauses (including Schedules 1 and 2) are incorporated by reference into the Data Processing Agreement and are effective from the DPA Effective Date.

Clause 1 - Definitions

For the purposes of the Clauses:

a. **Personal data**, **special categories of data**, **process/processing**, **controller**, **processor**, **Data Subject** and **Supervisory Authority** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
b. **Data Exporter** means the controller who transfers the personal data;
c. **Data Importer** means the processor who agrees to receive from the Data Exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25 (1) of Directive 95/46/EC;
d. **Subprocessor** means any processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any other subprocessor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
e. **Applicable data protection law** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the Data Exporter is established;
f. **Technical and organisational security measures** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 - Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Schedule 1 which forms an integral part of the Clauses.

Clause 3 - Third-party beneficiary clause

1. The Data Subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The Data Subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has

ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the Data Subject can enforce them against such entity.

3. The Data Subject can enforce against the Subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the Data Subject can enforce them against such entity. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by national law.

Clause 4 Obligations of the Data Exporter

The Data Exporter agrees and warrants:

a. That the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the Data Exporter is established) and does not violate the relevant provisions of that State;
b. That it has instructed and throughout the duration of the personal data processing services will instruct the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses;
c. That the Data Importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Schedule 2 to the Clauses;
d. That after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
e. That it will ensure compliance with the security measures;
f. That, if the transfer involves special categories of data, the Data Subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
g. To forward any notification received from the Data Importer or any Subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the Data Exporter decides to continue the transfer or to lift the suspension;
h. To make available to the Data Subjects upon request a copy of the Clauses, with the exception of Schedule 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
i. That, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a Subprocessor providing at least the same level of protection for the personal data and the rights of Data Subject as the Data Importer under the Clauses; and

j. That it will ensure compliance with Clause 4(a) to (i).

The Data Exporter acknowledges that its data will be hosted in the Google's data centers of Google Inc. and/or one or more of its affiliated entities (collectively, "Google") (and not by the Data Importer) and, as a consequence, that most of the technical and organisational security measures relating to the Data Importer's data (as notably referred to in paragraphs 4c., 4d., 4e. and 4h. above) will be provided by the applicable Google entity under its own liability. Accordingly, and notwithstanding any other provision in these Clauses, the Data Importer disclaims any and all responsibility in relation to any acts and/or omission of Google, including notably (without limitation) for such Google technical and organisational security measures as listed for information purposes only and without any representation in Schedules 1 and 2.

Clause 5 - Obligations of the Data Importer

The Data Importer agrees and warrants:

a. To process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;
b. That it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Data Exporter as soon as it is aware, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;
c. That it has implemented the technical and organisational security measures specified in Schedule 2 before processing the personal data transferred;
d. That it will promptly notify the Data Exporter about:
    i. Any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
    ii. Any accidental or unauthorised access; and
    iii. Any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorised to do so;
e. To deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal Data Subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
f. At the request of the Data Exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the supervisory authority;
g. To make available to the Data Subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Schedule 2 which shall be replaced by a summary description of the security measures in those cases where the Data Subject is unable to obtain a copy from the Data Exporter;
h. That, in the event of sub-processing, it has previously informed the Data Exporter and obtained its prior written consent;
i. That the processing services by the Subprocessor will be carried out in accordance with Clause 11;

j. To send promptly a copy of any Subprocessor agreement it concludes under the Clauses to the Data Exporter.

Clause 6 - Liability

1. The parties agree that any Data Subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or Subprocessor is entitled to receive compensation from the Data Exporter for the damage suffered.
2. If a Data Subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or his Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the Data Subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The Data Importer may not rely on a breach by a Subprocessor of its obligations in order to avoid its own liabilities.
3. If a Data Subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the Subprocessor agrees that the Data Subject may issue a claim against the data Subprocessor with regard to its own processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The liability of the Subprocessor shall be limited to its own processing operations under the Clauses.
4. Without prejudice to paragraphs 1, 2 and 3 of Clause 6, each party's aggregate liability to the other under or in connection with these Clauses (whether in contract, tort or otherwise) is limited to the amount paid for the services by Customer which is party to the Agreement in the 12 months immediately preceding the event (or first in a series of connected events) giving rise to the liability.

Clause 7 - Mediation and jurisdiction

1. The Data Importer agrees that if the Data Subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the Data Subject;
   a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   b. to refer the dispute to the courts in the Member State in which the Data Exporter is established.
2. The parties agree that the choice made by the Data Subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 - Cooperation with supervisory authorities

1. The Data Exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of the Subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the applicable data protection law.

3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any Subprocessor preventing the conduct of an audit of the Data Importer, or any Subprocessor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9 - Governing Law

The Clauses shall be governed by the law of the Member State in which the Data Exporter is established.

Clause 10 - Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 - Sub-Processing

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor as are imposed on the Data Importer under the Clauses. Where the Subprocessor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the Subprocessor's obligations under such agreement.
2. The prior written contract between the Data Importer and the Subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the Data Subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established.
4. The Data Exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.

Clause 12 - Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the Data Importer and the Subprocessor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The Data Importer and the Subprocessor warrant that upon request of the Data Exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Schedule 1 to the Model Contractual Clauses

Data Exporter	The Data Exporter is the Customer legal entity that is a party to the Clauses.
Data Importer	The Data Importer is the Supplier, a global provider of a variety of technology services for businesses.
Categories of Data Subjects	The personal data transferred concern personal data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services and concerning the categories of Data Subjects listed in the DPA Appendix 1.
Categories of Data	The personal data transferred is personal data that will be Processed by Supplier including data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services as listed in the DPA Appendix 1
Special categories of data (if appropriate)	The personal data transferred concern the special categories of data transmitted or displayed by end users via the Service (defined below)
Processing operations	The personal data transferred will be subject to the following basic processing activities: - **Scope of Processing:** – The Clauses reflect the parties' agreement with respect to the processing and transfer of personal data specified in this Schedule pursuant to the provision of the "Service" as defined under the Agreement. – Personal data may be processed for the following purposes: (a) to provide the Service, (which may include the detection, prevention and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfil the obligations under the Agreement. – The Data Exporter instructs the Data Importer to process personal data in countries in which the Data Importer or its Subprocessors maintain facilities as necessary for it to provide the Service - **Term of Data Processing:** Data processing will be for the term specified in the Agreement. For the term of the Agreement, and for a reasonable period of time after the expiry or termination of the Agreement, the Data Importer will provide the Data Exporter with access to, and the ability to export, the Data Exporter's personal data processed pursuant to the Agreement - **Data Deletion:** For the term of the Agreement, the Data Importer will provide the Data Exporter with the ability to delete the Data Exporter's personal data from the Service. After termination or expiry of the Agreement, the Data Importer will delete the Data Exporter's personal data in accordance with the Agreement. - **Access to Data:** For the term of the Agreement, the Data Importer will provide the Data Exporter with the ability to correct, block, export and delete the Data Exporter's personal data from the Service in accordance with the Agreement.

	– **Subprocessors**: The Data Importer may engage Subprocessors to provide parts of the Service. The Data Importer will ensure Subprocessors only access and use the Data Exporter's personal data to provide the Service and not for any other purpose.

Schedule 2 to the Model Contractual Clauses

Description of the technical and organisational security measures implemented by the Data Importer in accordance with Clauses 4(c) and 5(c):

The Data Importer currently abides by the security standards in this Schedule 2. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a material degradation in the security of the Service during the term of the Agreement.

1. **Google Data Center & Network Security**
   a. Data Centers
      i. **Infrastructure**. Google maintains geographically distributed data centers. Google stores all production data in physically secure data centers.
      ii. **Redundancy**. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. Google performs certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.
      iii. **Power**. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.
      iv. **Server Operating Systems**. The servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used and enhance the security products in production environments.
      v. **Businesses Continuity**. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.
      vi. **Decommissioned Disks and Disk Erase Policy**. Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned

("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

b. Networks & Transmission
   i. **Data Transmission**. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.
   ii. **External Attack Surface.** Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.
   iii. **Intrusion Detection**. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google intrusion detection involves:
      1. Tightly controlling the size and make-up of the attack surface through preventative measures;
      2. Employing intelligent detection controls at data entry points; and
      3. Employing technologies that automatically remedy certain dangerous situations.
   iv. **Incident Response**. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.
   v. **Encryption Technologie**s. Google makes HTTPS encryption (also referred to as SSL or TLS) available.

2. **Google Access and Site Controls**
   a. Site Controls
      i. **On-site Data Center Security Operation**. Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.
      ii. **Data Center Access Procedures**. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii)

sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved.

iii. **On-site Data Center Security Devices**. Google's data centers employ an electronic card key and biometric access control system that are linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 90 days based on activity.

b. Access Control

i. **Infrastructure Security Personnel**. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of the Data Importer's security infrastructure and for responding to security incidents.

3. **Data**

a. Data Storage, Isolation & Authentication

i. The Data Importer stores data in a multi-tenant environment on Google servers. Data, the Service database and file system architecture are replicated between multiple geographically dispersed Google data centers. The Data Importer logically isolates data on a per end user basis at the application layer. The Data Importer also logically isolates the Data Exporter's data, and the Data Exporter will be given control over specific data sharing policies. The Data Importer logically separates the Data Exporter's data, including data from different end users from each other, and data for an authenticated end user will not be displayed to another end user (unless the former end user or administrator allows the data to be shared). A central authentication system is used across the Service to increase uniform security of data. The Data Exporter will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Service, will enable the Data Exporter to determine the product sharing settings applicable to end users for specific purposes. The Data Exporter may choose to make use of certain logging capability that the Data Importer may make available via the Service, products and APIs. The Data Exporter agrees that its use of the APIs is subject to the API terms of use.

b. Access Control.

i. Access Control and Privilege Management. The Data Exporter's administrators and end users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Service. Each application checks credentials in order to allow the display of data to an authorized end user or authorized administrator.

ii. Internal Data Access Processes and Policies – Access Policy. The Data Importer's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. The Data Importer designs its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during

processing, use and after recording.The Data Importer employs a centralized access management system to control personnel access to production systems, and only provides access to a limited number of authorized personnel. The Data Importer requires the use of unique user IDs, strong passwords; two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with the Data Importer's internal data access policies and training. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength.

4. **Personnel Security**
    a. The Data Importer personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. The Data Importer conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.
    b. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, the Data Importer's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling customer data are required to complete additional requirements appropriate to their role (eg. activate two factor authentication on their account, encrypt their computer's hard disk). The Data Importer's personnel will not process customer data without authorization.

5. **Subprocessor Security**: Prior to onboarding Subprocessors, the Data Importer conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once the Data Importer has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

6. **Data Privacy Officer**: the Data Privacy Officer of the Data Importer can be contacted at: legal@revevol.eu