

Data Processing Addendum

Version: 2

Date: [27 October, 2026]

This Data Processing Addendum, including the exhibits to it ("**DPA**"), is incorporated into the Master Services Agreement and the Individual Orders (together, the "**Agreement**") that are between you ("Customer" or "Controller") and Doodle AG with the business address of Werdstrasse 21, 8004 Zurich, Switzerland (together, with any subsidiaries and affiliated entities, collectively "**Doodle**" or "**Processor**") and sets forth additional terms that apply to the extent any information you provide to Doodle pursuant to the Agreement includes Personal Data (as defined below).

1. DEFINITIONS

- A. "**CCPA**" means the California Consumer Privacy Act (California Consumer Privacy Act of 2018, Cal. Civ. Code § [1798.100 - 1798.199.100]) and its implementing regulations, each as may be amended from time to time, including without limitation by the California Privacy Rights Act of 2020.
- B. "**Data Privacy Framework(s)**" means, as applicable, the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework, and the Swiss-US Data Privacy Framework developed by the US Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration permitting US based organisations participating in such Data Privacy Frameworks to receive Personal Data from the European Union / European Economic Area, the UK and Gibraltar, and Switzerland in compliance with applicable Data Protection Laws in those regions.
- C. "**Data Protection Laws**" means all applicable federal, state, and foreign data protection, privacy and data security laws, as well as applicable regulations and formal directives intended by their nature to have the force of law, all as amended from time to time, and when referring to Processor's processing of Personal Data, to the extent directly applicable to such processing, including, without limitation, the EU Data Protection Laws, UK Data Protection Laws, the Swiss Data Protection Laws, the Privacy Act 1988, the Personal Information Protection and Electronic Documents Act, and the CCPA.
- D. "**Data Subject**" means the individual or consumer to whom Personal Data relates.
- E. "**Data Subject Request**" means a request by a Data Subject to exercise rights afforded by Data Protection Laws with respect to the Data Subject's Personal Data.
- F. "**EU Data Protection Laws**" means GDPR together with any applicable implementing legislation or regulations, as well as European Union or Member State laws, as amended from time to time.
- G. "**GDPR**" means the General Data Protection Regulation (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.)
- H. "**Party**" means either Customer or Doodle.
- I. "**Parties**" means collectively Customer and Doodle.
- J. "**Personal Data**" means any information relating to an identified or identifiable natural person that is Processed by Doodle on behalf of Customer in connection with providing the Services to Customer, when such information is protected as "personal data" or "personal information" or a similar term under Data Protection Law(s).

- K. **“Process”** or **“Processing”** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- L. **“Security Breach”** means a confirmed breach of Doodle’s information security measures leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data covered by this DPA.
- M. **“Services”** means the services provided by Doodle to Customer under the Agreement.
- N. **“Standard Contractual Clauses”** or **“SCCs”** means the model clauses for the transfer of Personal Data to processors established in third countries approved by the European Commission, the approved version of which is set out in the European Commission Implementing Decision 2021/914 of 4 June 2021 and at: https://eurlex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=e.
- O. **“Swiss Data Protection Laws”** means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in Switzerland, including the Swiss Federal Act on Data Protection dated 25 September 2020 and its ordinances.
- P. **“UK Data Protection Laws”** means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the United Kingdom (“UK”), including the United Kingdom GDPR and the Data Protection Act 2018.
- Q. **“UK GDPR”** means the United Kingdom General Data Protection Regulation, as it forms part of the law of the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018.
- R. The terms **“Processor”** and **“Controller”** shall have the meanings given to them under the applicable Data Protection Law. Any capitalised terms herein that are not defined in this DPA shall have the meanings associated with them in the Agreement and are hereby adopted by reference in this Addendum.

2. PROCESSING AND TRANSFER OF PERSONAL DATA

- A. **Customer Obligations.** Customer is, as between Customer and Doodle, the Controller of Personal Data and shall (a) determine the purpose and essential means of the Processing of Personal Data in accordance with the Agreement; (b) be responsible for the accuracy of Personal Data; and (c) comply with its obligations under Data Protection Laws, including, when applicable, ensuring Customer has a lawful basis to collect Personal Data, providing Data Subjects with any required notices, and/or obtaining the Data Subject’s consent to process the Personal Data.
- B. **Doodle Obligations.** Doodle is the Processor of Personal Data and shall (a) Process Personal Data on Customer’s behalf in accordance with Customer’s written instructions (unless waived in a written requirement) provided during the term of this DPA; and (b) comply with its obligations under Data Protection Laws. A description of the processing of Personal Data intended to be carried out under this DPA is set out in Annex 1. The Parties agree that the Agreement, including this DPA, together with Customer’s use of the Services in compliance with the Agreement, constitute Customer’s complete and final written instruction to Doodle in relation to the Processing of Personal Data, and additional instructions outside the scope of these instructions shall require a prior written and mutually executed agreement between Customer and Doodle. In the event Doodle reasonably believes there is a conflict with any Data Protection Law and Customer’s instructions, Doodle will inform Customer promptly and the Parties shall cooperate in good faith to resolve the conflict and achieve the goals of such instruction.
- C. **Data Use.** Doodle shall not use Personal Data, except for usage of Personal Data pursuant to Customer’s instructions, as permitted under the Agreement and as necessary to bring and defend claims, to comply with

requirements of the legal process, to cooperate with regulatory authorities, and to exercise other similar permissible uses as expressly provided under Data Protection Laws.

- D. **Location of Processing.** The Parties acknowledge and agree that processing of the Personal Data will occur in the European Union (EU), in Switzerland and perhaps (other) jurisdictions outside the residence of the Data Subjects, and Customer shall comply with all notice and consent requirements for such transfer and processing to the extent required by Data Protection Laws.
- E. **Return or Destruction of Data.** Doodle shall return or securely destroy Personal Data, in accordance with Customer's instructions, upon Customer's request or upon termination of Customer's account(s) unless Personal Data must be retained to comply with applicable law.

3. SWISS, EU, AND UK DATA PROTECTION LAWS

This Section shall apply with respect to Processing of Personal Data when such Processing is subject to the Swiss Data Protection Laws, EU Data Protection Laws, or UK Data Protection Laws.

- A. **Transfers of Personal Data.** Customer acknowledges and agrees that Doodle is located in Switzerland. Unless an exception set forth under the EU Data Protection Laws, the Swiss Data Protection Laws or the UK Data Protection Laws (as applicable) applies, transfers of Personal Data subject to the EU Data Protection Laws, the Swiss Data Protection Laws or the UK Data Protection Laws (as applicable) to a recipient in a jurisdiction not subject to an adequacy decision under applicable Data Protection Laws shall be governed by a data transfer agreement in a form prescribed by EU Data Protection Laws, the Swiss Data Protection Laws or the UK Data Protection Laws (as applicable) (e.g. Standard Contractual Clauses or equivalent), to the extent that the formalisation of such a document represents a valid means for the transfer of Personal Data subject to the EU Data Protection Laws, the Swiss Data Protection Laws or the UK Data Protection Laws (as applicable), or be conducted pursuant to any other valid transfer mechanism prescribed by EU Data Protection Laws, the Swiss Data Protection Laws or the UK Data Protection Laws (as applicable). To the extent that additional contractual, technical, or organisational measures are required by EU Data Protection Laws, the Swiss Data Protection Laws or the UK Data Protection Laws (as applicable) in order to lawfully carry out transfers of Personal Data subject to the EU Data Protection Laws, the Swiss Data Protection Laws or the UK Data Protection Laws (as applicable), each Party shall cooperate in good faith and implement and agree to such measures, including but not limited to the conclusion of the Standard Contractual Clauses (if required), as may be necessary to enable and maintain the lawfulness of such transfer.

A-1. Standard Contractual Clauses.

- a. Doodle (as "data exporter") and Customer (as "data importer") hereby enter into the Standard Contractual Clauses, Module 4, in respect of any transfers of Personal Data subject to the EU Data Protection Laws, the Swiss Data Protection Laws or the UK Data Protection Laws (as applicable) from Doodle to Customer. The Parties agree having access to and have knowledge of the Standard Contractual Clauses and hereby waive reproducing the Standard Contractual Clauses in this DPA. In the event of a conflict between this DPA and the Standard Contractual Clauses the Standard Contractual Clauses will prevail.
- b. In relation to the Standard Contractual Clauses, the Parties agree that Annex 1.A. of this DPA constitutes Annex I.A. of the Standard Contractual Clauses and Annex 1.B.-I. constitute Annex I.B. The Parties agree further that (i) Clause 7 applies; (ii) Clause 11(a) applies without the option; (iii) the Standard Contractual Clauses are governed by the laws of Switzerland, and the courts of Zurich are competent (Clauses 17 and 18).
- c. In relation to the Standard Contractual Clauses, where a transfer from Doodle to Customer is subject to the Swiss Data Protection Laws, (i) references to the law of the European Union are construed to include a reference to the Swiss Federal Data Protection Act ("FDPA"); (ii) Switzerland will be deemed to be a "member state" and references to a "member state" will be construed to include Switzerland; (iii) terms used in the Standard Contractual Clauses that are defined in the FDPA will be construed as under the FDPA.

- d. In relation to the Standard Contractual Clauses, where a transfer from Doodle to Customer is subject to the UK Data Protection Laws, such Clauses shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("UK IDTA"), and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is hereby completed as follows:
 1. For Table 1: the Parties' fields will be deemed to be pre-populated with the exporter and importer parties set out Annex 1.A hereto;
 2. For Table 2: said Clauses including the Appendix Information and with only the modules, clauses or optional provisions of the Clauses listed above for the EU and Switzerland, brought into effect for the purpose of the UK IDTA;
 3. For Table 3: the Appendix Information is set out in the following:
 - i. Annex IA: List of Parties: as set out in Annex 1.A hereto;
 - ii. Annex IB: Description of Transfer: as set out in Annex 1.B hereto;
 - iii. Annex II: N/A;
 4. For Table 4: either of them may end the UK IDTA in accordance with the provisions of Section 19 of the UK IDTA.
- B. **Obligations.** Doodle shall: (i) assist Customer, to a reasonable extent, in complying with its obligations pursuant to Articles 32 to 36 of GDPR, their equivalent under UK Data Protection Laws or their equivalent under Swiss Data Protection Laws, as applicable a); (ii) maintain a record of all categories of Processing activities carried out on behalf of Customer in accordance with Article 30(2) of the GDPR or their equivalent under UK Data Protection Laws or their equivalent under Swiss Data Protection Laws as applicable; and (iii) cooperate, on request, with an EU, UK or Swiss supervisory authority, as applicable regarding the performance of the Services.

4. CCPA

- A. **CCPA.** This Section applies to Doodle's, and Doodle acts as Customer's Service Provider (except as otherwise provided in this Section) with respect to, Processing of Personal Data subject to the CCPA. Customer discloses the Personal Data to Doodle, and Doodle shall Process such Personal Data only for the purposes as set out in this Agreement, including this DPA. To the extent there is a conflict between the terms of in this Section, on the one hand, and the Agreement, on the other hand, the terms set forth in this Section shall prevail. All capitalized terms used in this Section but not defined in the Agreement shall have the meaning given to them in the CCPA, unless otherwise stated.
- B. Doodle shall not:
 - a. Sell or Share the Personal Data;
 - b. retain, use, or disclose the Personal Data (i) for any purpose, including a Commercial Purpose, other than the Business Purposes as set out in the Agreement or reasonably related to the Services, or other than as otherwise permitted by the CCPA, or (ii) outside of the direct business relationship between the Parties, unless expressly permitted by the CCPA;
 - c. combine the Personal Data with personal data that Doodle receives from, or on behalf of, another person or persons, or collects from its own interaction with the Consumer, provided that Doodle may combine Personal Data to perform any Business Purpose as permitted by the CCPA.
- C. Doodle shall comply with obligations applicable to it as a Service Provider under the CCPA, and shall provide Personal Data with the same level of privacy protection as is required of Business by the CCPA.
- D. Customer shall have the right to take reasonable and appropriate steps to help ensure that Doodle uses the Personal Data in a manner consistent with Customer's obligations under the CCPA. The process for such steps shall be as set out in Section 8 below.
- E. Doodle shall notify Customer if it makes a determination that it can no longer meet its obligations as a Service Provider under the CCPA. If Doodle so notifies Customer, Customer shall have the right to take

reasonable and appropriate steps to stop and remediate unauthorised use of Personal Data.

- F. Doodle may engage a sub-processor to assist in Processing the Personal Data for a Business Purpose on behalf of Customer pursuant to a written (text form is sufficient) contract binding on the sub-processor that complies with the CCPA.
- G. To the extent that Customer discloses, shares, or otherwise makes available Personal Data to Doodle, Customer does so for the limited and specified Business Purpose(s) as described in Annex 1.
- H. To the extent that Customer discloses or otherwise makes available Deidentified data to Doodle, or Doodle Deidentifies Personal Data, Doodle agrees to (i) take reasonable measures to ensure that the Deidentified data cannot be associated with an individual or household; (ii) publicly commit to maintain and use the Personal Data in Deidentified form and not to attempt to reidentify the Personal Data, and (iii) contractually obligate any further recipient to comply with all provisions of this paragraph H.
- I. Doodle shall provide reasonable assistance to Customer in ensuring compliance with Customer's obligations to carry out risk assessments and Cybersecurity Audits, and to comply with Customer's requirements with respect to Automated Decision-Making Technologies, considering the nature of the Processing and the information available to Doodle.
- J. The Parties agree that no Sale or Share of Personal Data is intended as part of this Agreement, and the Parties agree that any provision of Personal Data by one Party to the other under this Agreement is necessary to perform a Business Purpose as described in Section 9 below or Annex 1, and is not part of, and is explicitly excluded from, the exchange of consideration, or any other thing of value, between the Parties.

5. SUB-PROCESSORS

- A. **Sub-processor List.** Customer consents to Doodle's use of sub-processors who may Process Personal Data on behalf of Customer to help Doodle provide the Services. [The list of Doodle's current sub-processors is available here.](#) Doodle may update its list of sub-processors from time to time, and shall make available any updates to such list online and give notice to Customer. Customer may object in writing within two (2) weeks from the notification for good cause. If Customer objects, the Parties shall negotiate in good faith to find a solution. If the Parties cannot agree on a solution within two (2) months from the notification of the objection, either Party may terminate the affected Individual Order by giving written notice within two (2) weeks following the expiry of the negotiation period.
- B. **Sub-processor Agreements.** Doodle shall enter into a written (text form is sufficient) agreement with any such sub-processor containing data protection obligations that are at least as restrictive as its obligations in this DPA.

6. DATA PROTECTION

- A. **Data Security.** Doodle will utilise commercially reasonable technical and organisational measures appropriate to the nature of the Personal Data to maintain the security, confidentiality, and integrity of the Personal Data, and to protect the Personal Data from unauthorised or illegal access, destruction, use, modification, or disclosure. Doodle shall implement and maintain at least the technical and organisational measures set out in Annex 2.
- B. **Authorised Personnel.** Doodle shall ensure that Doodle's employees, contractors, agents, and auditors who need to know or otherwise access Personal Data for the purposes of enabling Doodle to perform its obligations under the Agreement are under a duty of confidentiality with respect to the Personal Data.

- C. **Security Breaches.** Upon becoming aware of a Security Breach, Doodle will promptly: (i) notify Customer of the Security Breach; (ii) investigate the Security Breach; (iii) provide Customer with necessary details about the Security Breach as required by applicable law; and (iv) take reasonable actions to prevent a recurrence of the Security Breach. Doodle will make available relevant records and other materials related to the Security Breach's effects on Customer to the extent required to comply with Data Protection Laws, subject to any confidentiality obligations binding on Doodle under any applicable laws or contract.

7. ASSISTANCE

- A. **Processor Assistance.** Upon Customer's written request, Doodle shall provide reasonable assistance to Customer as necessary in order to assist Customer with meeting its obligations under Data Protection Laws, including by providing information to Customer about Doodle's technical and organisational security measures, and as needed to complete data protection assessments (the process for which is set out in Section 8 below).
- B. **Data Subject Requests.** If an invitee, a Customer employee, or other applicable Data Subject makes a Data Subject Request to Doodle, Doodle will advise the Data Subject to submit their request directly to the Doodle customer who is the applicable Controller of that Personal Data, and will inform Customer of such request if the Data Subject identifies Customer as the applicable Controller to Doodle. Customer is responsible for Data Subject Requests. Doodle shall provide full cooperation and assistance to the Controller in relation to any request by Data Subjects to have access to Personal Data held about them or in relation to any other request, allegation or complaint by a competent authority or Data Subject, including notifying the Controller in writing without undue delay of receipt of any such notice or request. Contact information for Data Subject Requests can be found on [our website](#).
- C. **Costs.** If Doodle determines in good faith that a request for assistance under this Section is unreasonable, overly burdensome, and outside of industry expectation for assistance with each respective matter, the Parties will agree in good faith on costs to be paid by Customer to Doodle for such assistance.

8. AUDITS

Within thirty (30) days of Customer's written request, and no more than once annually, Doodle shall make available to Customer (or a mutually agreed upon third-party auditor) information reasonably necessary to demonstrate Doodle's compliance with the obligations set forth in this DPA in the form of its most recent third party audit or certification report(s) (such as SOC 2 or Cloud Verify). If, after receiving the report(s), Customer in its reasonable judgement determines that further information is needed to confirm that Doodle is meeting its obligations in this DPA or for Customer to complete a data protection assessment, Customer may request in writing such additional information. The Parties will then work together in good faith to agree upon the additional information which Doodle shall provide, and Doodle will provide the agreed upon information. Where applicable Data Protection Law requires the right to on-site inspections, Doodle shall permit Customer to conduct such inspections. All information provided by Doodle under this Section is considered Doodle's Confidential Information and is subject to the confidentiality obligations set forth in the Agreement.

9. DOODLE'S ROLE AS A CONTROLLER

The Parties acknowledge and agree that Doodle processes certain personal data as a Controller which is described in, and processes it in accordance with, our Privacy Notice for the following purposes when EU, UK or Swiss Data Protection Laws apply to such personal data: (i) to manage the relationship with Customer, including creating customer accounts, handling billing, and performing sales and marketing activities; (ii) for purposes related to Doodle's internal business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of personal data to which Doodle is subject; (vi) to develop, improve, and understand usage of its

products and services, and (vii) as otherwise permitted under Data Protection Laws and as set out in Doodle's Privacy Notice.

10. MISCELLANEOUS

- A. **Conflict.** In the event of any conflict or inconsistency between this DPA and Data Protection Laws, Data Protection Laws shall prevail. In the event of any conflict or inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail solely to the extent that the subject matter concerns the processing of Personal Data.
- B. **Amendments.** This DPA shall not be modified except by a written instrument signed by the Parties. To the extent that it is determined by any data protection authority that the Agreement or this DPA is insufficient to comply with Data Protection Laws or changes to Data Protection Laws, Customer and Doodle agree to cooperate in good faith to amend the Agreement or this DPA or enter into further mutually agreeable data processing agreements in an effort to comply with all Data Protection Laws.
- C. **Liability.** Each Party's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the limitations of liability contained in the Agreement. For the avoidance of doubt, each reference herein to the "DPA" means this DPA including its exhibits and annexes.
- D. **Governing Law and Arbitration.** For the avoidance of doubt, Section 16.1 of the Master Services Agreement ("Governing Law and Arbitration") applies to this DPA.
- E. **Entire Agreement.** This DPA is without prejudice to the rights and obligations of the Parties under the Agreement which shall continue to have full force and effect. This DPA together with the Agreement is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the Parties with respect to such subject matter.

ANNEX 1: SCOPE OF PROCESSING

A. List of parties

a. Controller.

- i. Controller is the Customer.
- ii. Address: the Customer's address set out in the Agreement.
- iii. Contact person's name, position, and contact details are as set out in the order form.
- iv. Relevant activities: activities necessary to provide the Services described in the Agreement.
- v. Signature and date: Customer is deemed to have signed this Annex I by entering into the Master Services Agreement.

b. Processor.

- i. The Processor is Doodle AG.
- ii. Address: Werdstrasse 21, 8004 Zurich, Switzerland
- iii. Contact persons' name, position, and contact details: 1. Head of IT Operations & IT Security, security@doodle.com. 2. Doodle AG's DPO: Elena Frahm TÜV Informationstechnik GmbH Am TÜV 1 45307 Essen Germany Email: privacyguard@tuvit.de
- iv. Relevant activities: Activities necessary to provide the Services described in the Agreement.
- v. Signature and date: Doodle is deemed to have signed this Annex I by entering into the Master Services Agreement.

B. Categories of Data Subjects whose Personal Data is processed. Customer may submit Personal Data to Doodle, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects: (i) Customer's (and Customer's Affiliates') end-users as permitted in the Agreement, including employees, contractors, representatives, and agents, and (ii) persons with whom Customer (and Customer's Affiliates) is scheduling appointments and meeting with through use of Doodle's services which may include its representatives, business partners, collaborators, job candidates, customers, and potential customers.

C. Categories of Personal Data processed. Customer may submit Personal Data to Doodle, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: First and last name; Title; Position; Employer; Contact information (company, email, phone, physical business address); Personal Data contained in connected calendar event details; Approximate location and/or time zone; and other data in an electronic form used by Customer in the context of the Services.

D. Sensitive data transferred (if applicable). Sensitive data may be transferred in certain use cases of the Services such as racial or ethnic origin, trade union membership or data relating to health.

E. The Frequency of the Transfer. Continuous.

F. Subject matter/Nature of the processing. The processes may include collection, storage, retrieval, consultation, use, erasure, or destruction, disclosure by transmission, dissemination, or otherwise making available Customer's Personal Data as necessary to provide the Services in accordance with Customer's instructions, including related internal purposes where permitted by applicable laws (such as quality control, troubleshooting, information security, prevention and detection of spam, fraud, and abuse and product development and improvement).

- G. **Purpose(s) of the data transfer and further processing.** The objective of the processing of Personal Data by Doodle is the performance of the contractual Services under the Agreement with Customer.
- H. **The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period.** Personal Data is retained for as long as is reasonably necessary to fulfil the purposes for which the data was collected, to perform our contractual and legal obligations, and for any applicable statute of limitations periods for the purposes of bringing and defending claims.
- I. **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.** The subject matter and nature of the processing by sub-processors is as set out in the sub-processor list here. The duration of the processing by subprocessors shall be for as so long as Doodle provides the Services under the Agreement to Customer.
- J. **Business Purposes.** (1) Helping to ensure security and integrity of the Services (to the extent the use of the relevant Personal Data is reasonably necessary and proportionate for these purposes). (2) Debugging to identify and repair errors that impair existing intended functionality of the Services. (3) Performing the Services on behalf of the Customer, including providing support service to Authorized Users, verifying Customer Authorized User information, and providing data storage. (4) Undertaking internal research for technological development and demonstration of the Services.

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES

Doodle implements and maintains at least the technical and organisational measures set out in this Annex. Doodle's sub-processors implement and maintain technical and organisational measures that provide at least the same level of protection as Doodle's measures, even if such measures are not identical.

- A. **Confidentiality**
(Article 32(1)(a-b) of the GDPR or their equivalent under applicable Data Protection Laws)
 - a. **Physical Access Control.** Measures to prevent unauthorised persons from accessing data processing equipment with which data are processed or used:
 - Doodle deploys video management and physical access control systems across its offices, to prevent non-authorized persons (i.e. without proper access privileges) from accessing data processing equipment.
 - b. **Electronic Access Control.** Measures to prevent the use of data processing systems by unauthorised persons:
 - Access is restricted based on the principle of least privilege and need to know.
 - Doodle uses an identity and access management platform, username/password, SSO, and MFA to restrict access.
 - Doodle has a written password policy that is matched and enforced using the identity management service application password policy.
 - All Doodle laptops are encrypted using the File Storage Application.
 - Customer data is encrypted in the cloud using the Cloud Environment Application native AES-256 block cipher encryption and keys are managed via the Cloud Environment Application Key Management Service (KMS).
 - Doodle uses TLS 1.2 or higher to encrypt customer data in transit.
 - c. **Internal Access Control.** Measures to prevent that those authorised to use a data processing system can only access the data subject to their access authorisation and that data cannot be read, copied, modified or removed without authorisation during processing, use and after storage:

- Customer data is encrypted in the cloud using the Cloud Environment Application native AES-256 block cipher encryption and keys are managed via the Cloud Environment Application Key Management Service (KMS).
- Doodle uses TLS 1.2 or higher to encrypt customer data in transit.
- Segregation of duties is explicitly addressed in the Access Control Policy which contains a high-level explanation of the company's access segregation methodology.
- Logical access rights are segregated through Group permissions in the identity management service application.
- Doodle performs periodic reviews of access rights to enforce segregation of duties.
- Doodle utilizes the endpoint protection platform to monitor internal endpoints.

d. **Isolation Control.** Measures to prevent that data collected for different purposes can be processed separately:

- Access to Customer systems and configuration data is restricted to approved Doodle personnel.
- Production access is restricted to authorized personnel, with all code deployments and emergency fixes governed by mandatory peer reviews, automated CI/CD approval workflows, and ticketed change management processes.
- Doodle maintains a distinct Guest network and utilizes an MDM solution to rotate and push hidden passwords for the internal wireless network every six months, ensuring strict access demarcation.

e. **Pseudonymisation and Encryption.** Processing of personal data in such a way that data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and appropriate technical and organisational measures are taken:

- All Doodle laptops are encrypted using the File Storage Application.
- Doodle uses TLS 1.2 or higher to encrypt customer data in transit.
- Customer data is encrypted in the cloud using the Cloud Environment Application native AES-256 block cipher encryption and keys are managed via the Cloud Environment Application Key Management Service (KMS).
- Access to encryption keys is strictly governed by the principle of least privilege, restricted to a limited number of authorized personnel within Doodle.

B. Integrity

(Article 32(1)(b) of the GDPR or their equivalent under applicable Data Protection Laws)

a. **Transfer control.** Measures to prevent that data can be read, copied, altered or removed by unauthorised persons during electronic transmission or during their transport or storage on data carriers:

- All Doodle laptops are encrypted using the File Storage Application.
- Customer data is encrypted in the cloud using the Cloud Environment Application native AES-256 block cipher encryption and keys are managed via the Cloud Environment Application Key Management Service (KMS).
- Doodle uses TLS 1.2 or higher to encrypt customer data in transit.

b. **Input and disclosure control.** Measures to make it possible to check retrospectively whether and by whom data has been entered into, modified, disclosed (if applicable, to whom) and removed from the data processing systems:

- Doodle maintains comprehensive logs for all production environments. These logs are stored in a centralized repository that is logically separated from production systems to prevent tampering and ensure forensic integrity.
- All access and activity logs are retained for a minimum of one year, for compliance auditing and security monitoring purposes.

c. **Storage control:** Measures to prevent unauthorised persons to read, copy, alter, move, delete or destroy stored data:

- Customer data is managed, processed, and stored following the relevant data protection and other regulations formally established in our policies.
- Doodle follows a Role-Based Access Control (RBAC) policy as stated in Doodle's internal policies.
- Administration rights are restricted to accounts only accessible by Doodle's technical services team to which the administration role has been approved and granted through change control procedures.

C. Availability and resilience

(Article 32(1)(c) of the GDPR or their equivalent under applicable Data Protection Laws)

- a. **Availability control:** Measures to protect data against accidental destruction or loss:
- As a cloud-first organization, all data is hosted on high-availability cloud infrastructure with built-in redundancy across multiple availability zones.
- b. **Rapid recoverability:** Measures to enable rapid restore of data in the event of a physical or technical incident.
- Doodle performs daily full backups of its cloud infrastructure. • Internal backups are encrypted in transit and at rest. For in transit, Doodle uses a minimum of TLS 1.2 and for at rest encryption Doodle uses an industry standard AES-256 encryption algorithm.
- c. **System security:** Measures to adapt operating systems and application software to new security standards and resolve critical vulnerabilities:
- Doodle's Patch Management Policy governs a centralized ecosystem where endpoints are patched via mobile device management automation application and the cloud management application, infrastructure is managed through the Cloud Environment Application Patch Manager, and versioning releases are deployed via the App – Dev tool, ideally incorporating pre-production testing to evaluate patches before full deployment.
 - Doodle frequently scans its internal and public facing infrastructure for common vulnerabilities and exposures.

D. Procedures for regular review, assessment and evaluation

(Article 32(1)(d) of the GDPR or their equivalent under applicable Data Protection Laws)

a. **Data protection management:**

- Doodle has policies, procedures and standards aiming that customer personal data is handled responsibly and in compliance with data protection principles, laws, and regulations applicable to Doodle.
- Doodle has published and implemented an Information Classification Policy which addresses information classification and encryption. Staff and customer personal data are encrypted based on the policy.
- All staff laptops are encrypted using the File Storage Application.
- On an ongoing basis, Doodle delivers privacy awareness training across its staff population and, where permitted, records completion.
- Doodle reviews and records where and how its products and services collect, use, retain, and dispose of personal data. Risks are identified, recorded, and mitigated.

- Doodle is transparent about how it collects, processes, retains, and deletes personal data. The personal data Doodle collects, uses, processes and shares depends on the particular services that have been requested and/or activities being carried out. For more information, please see our Privacy Policy.
 - Doodle uses the personal data it collects in accordance with the relevant data protection rules and regulations applicable to Doodle. Doodle is clear about the reasons it collects and uses personal data and in a manner that is consistent with those purposes.
 - Customer data is further secured by a SDLC process that implements security best practices and controls for its applications such as AES 256-bit encryption for data at rest, monitoring and logging, vulnerability management and system hardening.
 - Doodle leverages an integrated platform for security awareness training combined with simulated phishing attacks on a regular basis for all its employees.
 - On an annual basis, Doodle completes an independent external audit based on the requirements of the trust services principles of AICPA's SOC 2 Type II. Doodle has also achieved MSP Alliance Cyber Verify Level 3, which means that critical areas of our cloud service operations, including data privacy, network security, availability and uptime, disaster recovery plans, scalability and compliance have been audited and deemed to meet industry regulations.
 - To fulfill the requirements of the GDPR, Doodle has formally appointed an external Data Protection Officer (DPO) to provide independent oversight and continued integrity of its personal data processing activities.
 - Doodle maintains a formalized process for handling data subject requests to permit compliance with applicable statutory rights of access, rectification, and erasure within the mandated regulatory timelines.
- b. **Incident response management:**
- Doodle has a Business Continuity Plan, Security Incident Response Plan, and Security Incident Response Procedures and Data Breach Management Policy and Procedures that are tested annually.