DASHLANE

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") amends and is incorporated into the Dashlane Business Terms and Conditions (the "**Terms**") between Client and Dashlane USA, Inc. (or Dashlane SAS, where applicable) (each, together with all affiliates, "**Dashlane**") only if Client or its Users provide Dashlane with Covered Personal Data (as defined below) in connection with Client's receipt of the Services. Capitalized terms used but not defined in this DPA have the meanings provided in the Terms. This DPA will control if there is any inconsistency between this DPA and the Terms.

1. **Definitions.**

(a) "**Data Protection Legislation**" means (a) the European Directive 2002/58/EC, and any legislation or regulation implementing or made pursuant to it, or which amends or replaces any of such legislation or regulation, including the General Data Protection Regulation EU 2016/679 (the "**GDPR**"), (b) the California Consumer Protection Act (the "**CCPA**") and (c) other laws and regulations that grant individuals analogous rights to those provided under the CCPA and GDPR..

(b) "**Covered Personal Data**", "**Data Processor**", "**Data Subject**", "**Data Controller**", "**Controller**", "**Processor**", "**Processing**", "**Subprocessor**", and "**Supervisory Authority**" have the meanings provided in the Data Protection Legislation.

2. **General.**

(a) The parties acknowledge that, due to the nature of the Services, Client is the Controller with respect to Covered Personal Data in the "business" space of the Services, while Dashlane is the Controller with respect to Covered Personal Data in a User's "personal" space of the Services. Client is neither a Data Controller nor a Data Processor of Covered Personal Data available in a User's "personal" space. Dashlane is a Data Controller of the Covered Personal Data in the Users' "personal" space, and the provisions of this DPA related to Processing apply only to Dashlane.

(b) Where Dashlane operates as a Data Processor, Dashlane will, to the extent legally permitted, promptly notify Client if Dashlane receives a request from a Data Subject to exercise any rights of the Data Subject with respect to their Personal Data, including the right of access, right to rectification, restriction of processing, erasure ("right to be forgotten"), data portability, objection to processing, or right not to be subject to automated individual decision making (each, "**Data Subject Request**"). Dashlane will reasonably assist Client where such assistance is required to respond to a Data Subject Request, to the extent Dashlane is legally permitted to do so and the response to the Data Subject Request is required under applicable laws.

(c) Each party will comply with its obligations under the Terms, its privacy policy or equivalent document ("**Privacy Policy**"), and the Data Protection Legislation in connection with its collection, provision, and Processing of Covered Personal Data.

(d) Client acknowledges that Dashlane is the Data Controller of each User's "personal" space and will determine the purpose and means of processing the Covered Personal Data of the User's "personal" space in accordance with the Data Protection Legislation, its Privacy Policy, and other relevant policies and procedures.

(e) Client acknowledges that the Terms as amended by this DPA set forth the purpose and means of Processing Covered Personal Data in connection with the Services.

(f) Dashlane will only Process the Covered Personal Data of the User's "business" space in accordance with (i) the Terms, and (ii) as further documented in other written instructions given by Client (which may be specific or of a general nature, or as otherwise notified by Client to Dashlane from time to time), where such instructions are consistent with the

Terms, this DPA, and Dashlane's then-current operating practices, unless Dashlane is required to process Covered Personal Data for any other purpose by European Union or member state law, or the laws of another jurisdiction with applicable to Covered Personal Data to which Dashlane is subject. Dashlane will inform Client of this requirement before Processing unless prohibited by applicable laws on grounds of public interest.

(g) Dashlane will promptly inform Client if, in Dashlane's view, any instructions Client provides regarding the processing of Covered Personal Data in the User's "business" space are inconsistent with the Data Protection Legislation.

(h) Client has or will obtain explicit consent to the Processing of Covered Personal Data of the Users' "business" space it makes available to Dashlane under the Agreement through its Privacy Policy, or otherwise has the right, subject to Article 6 of the GDPR, to provide such Covered Personal Data to Dashlane.

(i) Dashlane will obtain specific consent to Process Covered Personal Data for which Dashlane is the Controller via each User's acceptance of Dashlane's Privacy Policy, which is incorporated into the Terms and sets forth the statutory rights of all Users whose rights are determined by Data Protection Legislation with respect to their Covered Personal Data.

3. Security.

Dashlane will implement appropriate technical and organizational measures, including a written information security program that complies with applicable laws and regulations, including the Data Protection Legislation, designed to protect the security, integrity and confidentiality of Covered Personal Data, and protect against any unauthorized processing, loss, use, disclosure, acquisition of or access to any such data. For details of the security measures taken by Dashlane, see Exhibit A. Dashlane's obligations with respect to this Section 3 are further set forth in the Agreement.

4. Data Retention.

(a) Dashlane will not retain or process Covered Personal Data for longer than is necessary to carry out the purposes and obligations set out in the Agreement, provided, however, that it may retain or process Covered Personal Data following the expiration of the Agreement if permitted under a separate agreement, such as when a User establishes a personal account directly with Dashlane.

(b) Notwithstanding anything to the contrary herein, Dashlane may retain Covered Personal Data as required to comply with any applicable statutory or professional retention period.

5. Transfer of Covered Personal Data; Subprocessors.

(a) Client specifically approves Dashlane's affiliates as Subprocessors. In addition, Dashlane may transfer and otherwise Process Covered Personal Information outside the European economic area, the United Kingdom, and Switzerland, including by non-affiliated Subprocessors, provided that such transfer is made in compliance with the Data Protection Legislation, including where necessary, entering into the EU Model Standard Contractual Clauses for transferring Covered Personal Data outside of the European Economic Area (EEA) . All such transfers of Covered Personal Data to Dashlane are subject to the the model.

(b) Dashlane may use Subprocessors in connection with the Agreement, provided that (i) Dashlane has agreements in place with such Subprocessors, including DPAs where necessary, that comply with the Data Protection Legislation, and (ii) Dashlane obtains Client's prior consent to the use of such Subprocessors. A current list of Subprocessors is available here.

(c) Dashlane will provide Client with reasonable notice of any Subprocessor added during the Term. If Client objects to the use of such Subprocessor, Client must provide Dashlane with written notice of such objection as set forth in the Terms within ten (10) days. If Dashlane is unable, in its sole discretion, to not use such Subprocessor in connection with providing the Services to Client, Client's sole remedy, and Dashlane's entire obligation, will be to terminate the agreement (or, where applicable, the portion of the Services provided by such Subprocessor) and receive a pro-rata refund of any prepaid Fees attributable to the terminated Services.

6. **Cooperation with Authorities**.

At Client's request, Dashlane will make available information in its possession reasonably necessary to demonstrate Client's or Dashlane's compliance with the Data Protection Legislation requested in connection with investigations or audits conducted to demonstrate Client's or Dashlane's compliance (including any investigations or request by the relevant regulatory authorities) with the Data Protection Legislation.

7. **Amendments**.

Dashlane may modify Subprocessors at any time, but will provide you with reasonable advance notice of any such change as required by Section 5(c). When we make any modifications to the DPA, we will post the updated DPA on this page and inform you through the Services or via email, as applicable, and the revised DPA will only take effect during the next Renewal Term.

Exhibit A
Security Measures

1. Physical Security & Disaster Recovery

Dashlane Services are hosted on Amazon Web Services, which enforces strong physical security practices at its datacenters, details of which can be found here. As described in the whitepaper, AWS security measures include:

- Unmarked facilities;
- Strict physical access controls, including security staff, video surveillance, intrusion detection, and two-factor authentication;
- Logging and regular auditing of all employee access;
- Fire detection and suppression equipment;
- Fully redundant power supply, including the use of an uninterruptible power system and backup generators;
- Precise climate and temperature controls;
- Continuous monitoring and preventative maintenance of critical infrastructure; and
- Storage device decommissioning process using techniques detailed in the NIST 800-88 guidelines.

Dashlane offices have biometric access systems that track all employee access and allow role-based access to restricted areas.

2. Information and Data Security

- Dashlane's information security policy is reviewed by all new employees and available to all employees via Dashlane's internal communications system;
- Dashlane maintains a standing Risk Committee comprised of senior executives that meets monthly to monitor, track, and remediate identified risks across all areas of the business;
- Employees are made aware of any information security policy updates and other security-related process updates relevant to their functions;
- Dashlane's network, application(s), and other services are continuously monitored and subject to regular penetration testing;
- A private bug bounty service is used to identify vulnerabilities within Dashlane's systems;
- Dashlane's network and AWS instances are continuously monitored for malicious and unauthorized behavior;
- Dashlane's Services architecture incorporates privacy by design principles that prevent anyone other than the user (including Dashlane) from being able to access user data stored on the Services, as further described here.

3. Network Access

- Access to internal Dashlane services is only available at Dashlane facilities or through

Dashlane’s VPN;

- Access to production systems and other sensitive services is restricted to authorized employees only and all activities are logged and auditable;
- Two-factor authentication is used wherever available and for all internal services that have any sensitive information;
- Access to internal and production systems is provided on a least-privilege basis;
- Access rights are revoked as soon as an employee or contractor separates from Dashlane;
- Production and test instances are logically separated; and
- Usage information is logically separated from user information.

4. **Passwords**

- Employees are required to use strong, regularly changed, random, non-shared passwords for access to all Dashlane systems;
- Dashlane IT regularly tests internal Dashlane passwords; and
- Passwords to user accounts are not known to, stored by, or accessible to Dashlane. There is no master key or other decryption method available to Dashlane to access such information.

Exhibit B
Standard Contractual Clauses

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

The Client as identified pursuant to the "Terms" as defined above
hereinafter "data exporter")

and

Dashlane USA, Inc., with an address at 44 West 18th Street., New York, NY 10011
hereinafter "data importer"

each a "party"; together "the parties".

Definitions

For the purposes of the clauses:

(a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) "the data exporter" shall mean the controller who transfers the personal data;

(c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

(d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

(e) The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and docu- mentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any inde- pendent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions [1] of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data [2], or

(iii) the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: (iii)

Initials of data importer: Dp ;

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter’s country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

[1] “Relevant provisions” means those provisions of any authorisation or decision except for the enforcement provisions of any author- isation or decision (which shall be governed by these clauses).

[2] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated: as of the date of the Terms

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as infor- mation about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.
6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.
8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his

performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

(a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

(ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

(b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

(To be completed by the parties)

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects:
Employees, contractors…………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………….
…………………………………………………………………………………………………

Purposes of the transfer[s]

The transfer is made for the following purposes:
To provide the digital identity security and password management Services as described in the.. Terms.
…………………………………………………………………………………………………….
…………………………………………………………………………………………………

Categories of data

The Personal Data transferred concern the following categories of data:
Account data used to identify users of the Services and communicate with them as required ("Account Data"). Account Data includes business email of users
Name, business email, phone, and office location for administrators of Client accounts.

Recipients

The Personal Data transferred may be disclosed only to the following recipients or categories of recipients:
Affiliates of the data importer, entities identified as subprocessors by the data importer at https://www.dashlane.com/privacy/subprocessor…………………………………………………
…………………………………………………………………………………………………….

Sensitive Data (if appropriate)

The Personal Data transferred concern the following categories of Sensitive Data:
No Sensitive Data is requested, or required to provide the Services, or is processed by the data. importer as part of Account Data

Data protection registration information of Data Exporter (where applicable)

…………………………………………………………………………………………………
…………………………………………………………………………………………………

Additional useful information (storage limits and other relevant information)

…………………………………………………………………………………………………
…………………………………………………………………………………………………

Contact points for data protection enquiries

Data Importer Data Exporter

dpo@dashlane.com. As set forth in the Terms or Order Form
………………………………………… …………………………………………