DATA PROCESSING ADDENDUM

Updated: December 13, 2022

This Data Processing Addendum ("**DPA**") amends and is incorporated into the Dashlane BusinessTerms and Conditions (the "**Terms**") between Client and Dashlane USA, Inc., or Dashlane SAS, as applicable (together with all affiliates, "**Dashlane**") only if Client or its Users provide Dashlane with Personal Data subject to Applicable Data Protection Laws (as defined below) in connection with Client's receipt of the Services.

1. DEFINITIONS

The terms below have the following meanings:

a) "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

b) "**Applicable Data Protection Laws**" means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Personal Data under the Agreement, including the European Data Protection Laws, the CPRA, the Virginia Consumer Data Protection Act ("**VCPDA**") and any other such laws

c) "**CPRA**" means the California Consumer Protection Act of 2018, as amended by the California Privacy Rights Act of 2020, and any regulations promulgated thereunder.

d) **"Client Data**" means information provided or made available to Dashlane for Processing on Client's behalf to perform the Services.

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

f) "**European Data Protection Laws**" means the GDPR and other data protection laws and regulations of the European Union, its Member States, Switzerland, Iceland, Liechtenstein, Norway, and the United Kingdom, in each case, to the extent applicable to the Processing of Personal Data under the Agreement.

g) **"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as amended from time to time.

h) **"Information Security Incident"** means a breach of Dashlane's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Dashlane's possession, custody or control.

i) **"Personal Data"** means Client Data that is "personal data," "personal information," "personally identifiable information" or the equivalent as defined in Applicable Data Protection Law, provided that Personal Data does not include such information about Client personnel or representatives who are business contacts of Dashlane, where Dashlane acts as a controller of such information.

j) **"Processing"** means any operation or set of operations performed on Personal Data, such as collection, organization, storage, alteration, retrieval, use, disclosure, erasure or destruction.

k) **"Security Measures"** has the meaning given in Section 4(a).

l) **"Standard Contractual Clauses"** or "**SCCs**" means the mandatory provisions of Module 2 of the standard contractual clauses for the transfer of personal data to third countries in the form mandated by Regulation (EU) 2016/679, as set out in the European Commission's Implementing Decision 2021/914 of 4 June 2021, attached as Exhibit 4.

m) **"Subprocessors"** means third parties that Dashlane engages to Process Personal Data in relation to the Services.

n) **"Third Party Subprocessors"** has the meaning given in Section 6.

o) "**UK Addendum**" means the UK International Data Transfer Addendum to the Standard Contractual Clauses version B1.0 set out in Exhibit 5, as may be amended, replaced or superseded by the ICO from time to time (including when formally issued by the ICO under section 119A(1) Data Protection Act 2018).

p) "**UK GDPR**" means EU Regulation 2016/679 as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018.

The terms "controller," "data subject," "processor," and "supervisory authority" have the meanings given in the GDPR or the UK GDPR, as applicable. Capitalized terms that are used but not defined in this DPA have the meanings given in the Terms. For the purposes of the CPRA, as used herein, "controller" should be read as "business" and "processor " should be read as "service provider."

2. DURATION AND SCOPE OF DPA

a) This DPA will remain in effect so long as Dashlane Processes Personal Data, notwithstanding the expiration or termination of the Agreement (as defined below).

b) Exhibit 1 to this DPA applies solely to Processing subject to European Data Protection Laws. Exhibit 2 to this DPA applies solely to Processing subject to the CPRA if Client is a "business" or "service provider" (as defined in CPRA) with respect to such Processing.

c) The SCCs apply directly to Dashlane USA, Inc., where it is the Dashlane contracting entity. Where Dashlane SAS is the contracting entity, it represents and warrants that Dashlane USA, Inc. is bound to follow the SCCs pursuant to intercompany agreements between the Dashlane entities.

d) This DPA applies to Personal Data provided to Dashlane by Client, and Personal Data stored in the "business" space of the Services by Users. It does not apply to Personal Data stored in the "personal" space of the Services by Users, unless such Data is associated with a domain name owned by Client.

3. CLIENT INSTRUCTIONS

Dashlane will Process Personal Data only in accordance with Client's instructions and only for the purposes set forth in the Terms and the Order Form (or any other such equivalent documents entered into by Dashlane and the Client) (collectively, the "**Agreement**"). This DPA and the Agreement are a complete expression of such instructions, and Client's additional instructions will be binding on Dashlane only pursuant to an amendment to the Agreement or this DPA signed by both parties. Client instructs Dashlane to Process Personal Data to provide the Services as contemplated by the Agreement.

4. SECURITY

a) **Dashlane Security Measures**. Dashlane will implement and maintain technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data (the "**Security Measures**") as described in Exhibit 3. Dashlane may update the Security Measures from time to time, provided the updated measures do not decrease the overall protection of Personal Data.

b) **Security Compliance by Dashlane Staff**. Dashlane will ensure that its personnel who are authorized to access Personal Data are subject to appropriate confidentiality obligations and trained in the proper handling and safeguarding of Personal Data.

c) **Dashlane Security Assistance**. Dashlane will reasonably assist Client as necessary for Client to comply with its obligations regardmg Personal Data under Applicable Data Protection Laws, including Articles 32 through 34 of the GDPR or UKGDPR, as applicable.

d) **Information Security Incidents**. Dashlane will notify Client within 36 hours of any Information Security Incident of which Dashlane becomes aware. Such notifications will describe available details of the Information Security Incident, including mitigation efforts taken by Dashlane and steps Dashlane recommends Client take to address the Information Security Incident. Dashlane's notification of or response to an Information Security Incident is not an acknowledgement of any fault or liability with respect to such Information Security Incident.

e) Client's Security Responsibilities and Assessment

i. Client's Security Responsibilities. Client is solely responsible for its use of the Services, including (A) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data; (B) securing the account authentication credentials, systems and devices Client and its Users use to access the Services; and (C) backing up Personal Data.

ii. Client's Security Assessment. Client agrees that the Services, the Security Measures and Dashlane's commitments under this DPA are adequate to meet Client's needs, including with respect to any security obligations of Client under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Personal Data.

f) **Data Deletion**. Dashlane will delete all Personal Data on Dashlane's systems upon Client's request and after the end of the provision of Services, and will delete any copies thereof unless continued storage of Personal Data is required by (i) applicable laws of the European Union or its Member States or the United Kingdom, with respect to Personal Data subject to European Data Protection Laws, or (ii) Applicable Data Protection Laws, with respect

to all other Personal Data. Dashlane will comply with such instruction as soon as reasonably practicable and no later than 90 days after such expiration or termination. Note that, due to Dashlane's "Zero Knowledge" architecture, certain deletions of Personal Data stored within User accounts must be performed by Client and/ or Users. Dashlane will assist Client with this process as reasonably requested.

5. DATA SUBJECT RIGHTS

a) **Dashlane's Data Subject Request Assistance**. Dashlane will provide Client with assistance reasonably necessary for Client to perform its obligations under Applicable Data Protection Laws to fulfill requests by data subjects to exercise their rights under Applicable Data Protection Laws ("**Data Subject Requests**") with respect to Personal Data in Dashlane's possession or control.

b) **Client's Responsibility for Requests**. If Dashlane receives a Data Subject Request, Dashlane will advise the data subject to submit the request to Client and Client will be responsible for responding to the request and, as applicable, directing Dashlane to honor such request.

6. SUBPROCESSORS

a) **Consent to Subprocessor Engagement.** Client specifically authorizes the engagement of Dashlane's Affiliates as Subprocessors and generally authorizes the engagement of other third parties as Subprocessors ("**Third Party Subprocessors**") subject to the remainder of this Section 6.

b) **Information about Subprocessors.** Information about Subprocessors, including their functions and locations, is available here (as may be updated by Dashlane from time to time subject to the provisions of this Section 6) or on such other website address Dashlane may provide to Client from time to time (the "**Subprocessor Site"**).

c) **Requirements for Subprocessor Engagement.** Dashlane will only engage Third Party Subcontractors where such engagement is reasonably necessary to the performance of the Services, the Third Party Subprocessor is subject to obligations materially similar to those herein with respect to Client Personal Data and is prevented fro using the Personal Data made available to it for any purpose other than to provide the specified services to Dashlane, and Dashlane has undertaken commercially reasonable efforts to assess the Third Party Subprocessor's ability to properly protect the Personal Data it processes on Dashlane's behalf.
Dashlane will be liable for compliance by Subcontractors with the Terms and this DPA.

d) **Opportunity to Object to Subprocessor Changes.** When Dashlane engages any new Third Party Subprocessor after the effective date of the Agreement, Dashlane will notify Client of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) by updating the Subprocessor Site or by other written means. If Client objects to such engagement in a written notice to Dashlane within 15 days after being informed of the engagement on reasonable grounds relating to the protection of Personal Data, Client and Dashlane will work in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Client may, as its sole and exclusive remedy, terminate the Agreement and cancel the Services by providing written notice to Dashlane and pay Dashlane for all amounts due and owing under the Agreement as of the date of such termination.

7. REVIEWS AND AUDITS OF COMPLIANCE

Client may audit Dashlane's compliance with its obligations under this DPA up to once per year and on such other occasions as required by Applicable Data Protection Laws, including when mandated by Client's supervisory authority. Dashlane will provide Client or Client's supervisory authority with the information and assistance reasonably necessary to conduct the audit. Dashlane may object to any third-party auditor that, in Dashlane's reasonable opinion, is not independent, is a competitor of Dashlane, or is otherwise manifestly unsuitable. In such case, Client will appoint another auditor or conduct the audit itself. Client must submit a proposed audit plan to Dashlane at least two weeks before the proposed audit date, and any third-party auditor must sign a non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld). Dashlane will work with Client to agree on a final audit plan. The audit must be conducted during regular business hours, subject to the agreed final audit plan and Dashlane's safety, security and other relevant policies, and may not unreasonably interfere with Dashlane business activities. If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Client's audit request and Dashlane has confirmed there have been no known material changes in the controls audited since the date of such report, Client will accept such report in lieu of auditing such controls or measures. Client will promptly notify Dashlane of any non-compliance discovered during an audit and provide Dashlane any audit reports, unless prohibited by Applicable Data Protection Laws or otherwise instructed by

its supervisory authority. Client may use the audit reports only to meet Client's regulatory audit requirements and/or confirm compliance with the requirements of this DPA. Any audits are at Client's sole expense.

8. CLIENT RESPONSIBILITIES

Client will (a) comply with its obligations under Applicable Data Protection Laws, (b) ensure that its instructions in Section 3 comply with Applicable Data Protection Laws, and (c) provide all notices to, and obtain any necessary consents from, individuals to whom Personal Data pertains and all other parties as required by applicable laws or regulations for Client to Process Personal Data as contemplated by the Agreement.

9. MISCELLANEOUS

Except as expressly modified by this DPA, the provisions of the Terms remain in full force and effect. In the event of any conflict or inconsistency between this DPA and the Terms, this DPA will govern. Notwithstanding anything in the Agreement or any Order Form, the parties acknowledge that Dashlane's access to Personal Data is not part of the consideration exchanged by the parties in respect of the Agreement. Any notices required or permitted to be given by Dashlane to Client under this DPA may be given (a) in accordance with any notice clause of the Terms; (b) to Dashlane's primary points of contact with Client; or (c) to any email provided by Client for the purpose of providing it with Services-related communications or alerts. Client is solely responsible for ensuring that such email addresses are valid.

EXHIBIT 1 TO DPA
EU SPECIFIC PROVISIONS

1. **PROCESSING OF DATA**
   a) **Subject Matter and Details of Processin**g. The parties acknowledge and agree that (i) the subject matter of the Processing under the Agreement is Dashlane's provision of the Services; (ii) the duration of the Processing is from Dashlane's receipt of Personal Data until deletion of all Personal Data by Dashlane in accordance with the Agreement; (iii) the nature and purpose of the Processing is to provide the Services; (iv) the data subjects to whom the Personal Data pertains are employees, contractors, or otherwise permitted to use the Services on behalf of the Client; and (v) the categories of personal data are business contact information (e.g., emails), passwords, credentials and other information used by the data subjects on behalf of the Client of the data subjects.
   b) **Roles and Regulatory Compliance; Authorization**. The parties acknowledge and agree that (i) Dashlane is a processor of that Personal Data under European Data Protection Laws, (ii) Client is a controller (or a processor acting on the instructions of a controller) of that Personal Data under European Data Protection Laws, and (iii) each party will comply with the obligations applicable to it in such role under the European Data Protection Laws with respect to the Processing of that Personal Data. If Client is a processor, Client represents and warrants to Dashlane that Client's instructions and actions with respect to Personal Data, including its appointment of Dashlane as another processor, have been authorized by the relevant controller.
   c) **Dashlane's Compliance with Instructions**. Dashlane will Process Personal Data only in accordance with Client's instructions stated in this DPA, unless applicable European Data Protection Laws require otherwise, in which case Dashlane will so notify Client (unless that law prohibits Dashlane from doing so on important grounds of public interest).

2. **IMPACT ASSESSMENTS AND CONSULTATIONS**

Dashlane will reasonably assist Client in complying with its obligations under Articles 35 and 36 of the GDPR and/or the UK GDPR, as applicable, by (a) making available documentation describing relevant aspects of Dashlane's information security program and the security measures applied in connection therewith and (b) providing the other information contained in the Agreement, including this DPA.

3. **DATA TRANSFERS**
   a) **Data Processing Facilities.** Dashlane may, subject to Section 3(b), store and Process Personal Data in the United States or anywhere Dashlane or its Subprocessors maintains facilities.
   b) **Transfers out of the EEA**. If Client transfers Personal Data out of the EEA to Dashlane in a country not deemed by the European Commission to have adequate data protection, such transfer will be governed by the Standard Contractual Clauses attached as Exhibit 4 to this DPA. In furtherance of the foregoing, the parties agree that:
      i. Client will act as the data exporter and Dashlane will act as the data importer under the Standard Contractual Clauses;
      ii. for purposes of Appendix 1 to the Standard Contractual Clauses, the categories of data subjects, data, special categories of data (if appropriate), and the Processing operations will be as set out in Section 1(a) to this Exhibit 1;
      iii. for purposes of Appendix 2 to the Standard Contractual Clauses, the technical and organizational measures will be the Security Measures;
      iv. data importer will provide the copies of the subprocessor agreements that must be sent by the data importer to the data exporter pursuant to Clause 8.9(c) of the Standard Contractual Clauses upon data exporter's request, provided that data importer may remove or redact all commercial information or clauses unrelated the Standard Contractual Clauses or their equivalent beforehand;
      v. the audits described in Clauses 8.9 and 13 of the Standard Contractual Clauses will be performed in accordance with Section 7 of the DPA;
      vi. Client's authorizations in Section 6 of the DPA will constitute Client's prior written consent to the subcontracting by Dashlane of the Processing of Personal Data if such consent is required under Clause 8.8 of the Standard Contractual Clauses; and

vii. certification of deletion of Personal Data as described in Clause 8.5 of the Standard Contractual Clauses will be provided upon data exporter's request.

c) **Transfers out of the United Kingdom**. If Client transfers Personal Data out of the UK to Dashlane in a country not deemed by the UK Secretary of State to have adequate data protection, such transfer will be governed by the SCCS attached as Exhibit 4 to this DPA, as amended by the UK Addendum attached as Exhibit 5 to this DPA. The parties agree that the Part 1 tables in the UK Addendum will be deemed to be completed as follows (and that the tables do not need to be filled in for Exhibit 5 to be effective, where applicable):

i. Table 1 will be deemed completed with the relevant information set out in Annex I to the Standard Contractual Clauses;

ii. In Table 2, the first option will be selected and the relevant version of the Approved EU SCCs referenced in that option will be the Standard Contract Clauses referenced in Clause 3(b) above (incorporating the amendments to them set out in Clauses 3(b)(i) to (vii) inclusive;

iii. Table 3 will be deemed completed as set out in Clause 3(b)(ii) and 3(b)(iii) above, and the List of Subprocessors will be as detailed at Annex III of Exhibit 4; and

iv. Table 4 will be deemed completed such that the Exporter may end the UK Addendum as set out in Section 19 of Part 2 of the UK Addendum.

In there is any conflict or inconsistency between (a) this Exhibit 1 and any other provision of this DPA, this Exhibit 1 will govern (b) the Standard Contractual Clauses and any other provision of this Agreement, the Standard Contractual Clauses will govern, or (c) the UK Addendum and any other provision of the DPA or the Agreement, the UK Addendum will govern.

EXHIBIT 2 TO DPA
CALIFORNIA SPECIFIC PROVISIONS

1. For purposes of this Exhibit 2, the terms "business," "commercial purpose," "sell" and "service provider" will have the respective meanings given thereto in the CPRA, and "personal information" will mean Personal Data that constitutes personal information governed by the CPRA.

2. It is the parties' intent that with respect to any personal information, Dashlane is a service provider. Dashlane will not (a) sell any personal information; (b) retain, use, or disclose personal information for any purpose other than to provide the Services, including retaining, using, or disclosing the personal information except as necessary to provide the Services; or (c) retain, use or disclose the personal information outside of the direct business relationship between Dashlane and Client. Dashlane hereby certifies that it understands its obligations under this Section 2 and will comply with them.

3. Dashlane will not (i) sell or share Client Personal Data as such terms are defined under the California Consumer Privacy Act of 2018 (as amended by the CPRA) or any substantially similar law, nor (ii) use, retain, or disclose Client Personal Data (except where expressly required or permitted under applicable law) for any purpose other than the limited and specified business purposes as specified under the Agreement; or outside of its direct business relationship with Client. Where and to the extent required by applicable law (i) Dashlane will promptly notify Client if it can no longer meet its obligations under such law and (ii) Client will have the right, including in the event of such notice from Outreach, to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

4. The parties acknowledge that Dashlane's retention, use and disclosure of personal information authorized by Client's instructions documented in the DPA are integral to Dashlane's provision of the Services and the business relationship between the parties.

EXHIBIT 3 TO DPA
SECURITY MEASURES

1. Physical Security & Disaster Recovery

Dashlane Services are hosted on Amazon Web Services, which enforces strong physical security practices at its data centers, 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.
- A Risk Committee comprised of senior executives meets monthly to identify, monitor, track, and remediate risks across all areas of the business.
- Employees are made aware of information security policy updates and other changes to security-related processes relevant to their functions.
- Employees receive regular (at least annual) security training, and role-based training is performed when appropriate (e.g., upon promotion to new roles).
- Dashlane's network, application(s), and other services are continuously monitored.
- We have regular penetration testing and source code audits of the production environment performed.
- 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.
- All code is developed internally and subject to QA prior to release.
- Dashlane's Services architecture incorporates privacy by design principles that ensure that only Client Users and (in certain circumstances) Client IT Admins, can access user data stored on the Services. See this paper for more information.
- User Data is encrypted at all times when in transit to and from, and when stored on Dashlane servers.
- Behavioral Data (as defined in our Privacy Policy) is only available to Dashlane on a fully anonymized basis.
- Dashlane security conducts regular tests of internal system security and employee security awareness.

3. Network Access

- Access to internal Dashlane systems is only available at Dashlane facilities or through Dashlane's VPN.
- Access to production systems and other sensitive services is restricted to authorized employees, and all activities are logged and auditable;
- Two-factor authentication is mandated to access Dashlane internal systems and to access subprocessor systems that are used to process Personal Data;
- Access to internal and production systems is provided on a least-privilege basis.
- Access rights are revoked when an employee or contractor separates from Dashlane.

4. Passwords

- Employees are required to use strong, regularly changed, random, non-shared passwords for access to all Dashlane systems; and
- Dashlane IT regularly tests internal Dashlane passwords.

EXHIBIT 4 to DPA

STANDARD CONTRACTUAL CLAUSES
CONTROLLER TO PROCESSOR (2021)

SECTION 1
Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:
   (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Exhibit I.A (hereinafter each 'data exporter'), and
   (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

   have agreed to these standard contractual clauses (hereinafter: "**Clauses"**).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to herein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
   (iii) Clause 9(a), (c), (d) and (e);
   (iv) Clause 12(a), (d) and (f);
   (v) Clause 13;
   (vi) Clause 15.1(c), (d) and (e);
   (vii) Clause 16(e);
   (viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout

the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 15 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

  (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

  (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

  (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

  (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

  (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal

data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of France.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I TO THE STANDARD CONTRACT CLAUSES

A. LIST OF PARTIES

Data exporter(s): The Client as identified pursuant to the "Terms" as defined above

Activities relevant to the data transferred under these Clauses: Digital identity security and password management Services as described in the Terms

Role: Controller

Data importer(s): Dashlane USA, Inc., with an address at 44 West 18th Street, New York, NY 10011

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

Activities relevant to the data transferred under these Clauses: Digital identity security and password management Services as described in the Terms

Role: Processor

Date: as of the date of the Terms

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees and/or contractors of customers

Categories of personal data transferred

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.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No Sensitive Data is requested, or required to provide the Services, or is processed by the data. importer as part of Account Data. However, users of the service may choose to put Sensitive Data, including identification cards and financial information, on the Services (all such data stored on the Services, "**User Data**"). To ensure that User Data is only available to the user, Dashlane employs strict privacy-by-design principles (zero-knowledge architecture) that prohibit Dashlane and subcontractors from accessing User Data during processing. User information is encrypted at all times when on our servers, and each user's data is encrypted using a unique key that is not available to Dashlane. There is no master key or backdoor that allows Dashlane or any third party to access user data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

Account Data is used to administer accounts and provide user support; User Data is used to provide the Services functionality (autofill, password generation, etc.).

Purpose(s) of the data transfer and further processing

To provide the Services and support.

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 will be retained as long as necessary to fulfil the obligations set out in the Agreement, provided, however, that Dashlane may retain or process Account and User following the expiration of the Agreementif permitted under a separate agreement, such as when a User establishes a personal account directly with Dashlane. Notwithstanding anything to the contrary herein, Dashlane may retain Covered Personal Data as required to comply with any applicable statutory or professional retention period.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Affiliates of the data importer, entities identified as subprocessors by the data importer at https://www.dashlane.com/privacy/subprocessor

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

CNIL

ANNEX II TO THE STANDARD CONTRACT CLAUSES

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Exhibit 3 to the DPA: "Security Measures"

Furthermore:

As noted elsewhere, to ensure that User Data is only available to the user, Dashlane employs strict privacy-by-design principles (zero-knowledge architecture) that prohibit Dashlane and subcontractors from accessing User Data at any time. User information is encrypted at all times when on our servers, and each user's data is encrypted using a unique key that is not available to Dashlane. Decryption of User Data necessary to the operation of the Services occurs only on devices registered to the applicable user (i.e., all core user functionality runs locally). There is no master key or backdoor that allows Dashlane or any third party to access User Data.

Importer represents and warrants that:

1. Importer has not purposefully created backdoors or similar programming that could be used to access its systems or Personal Data,
2. Importer has not purposefully created or changed its business processes in a manner that facilitates access to its systems or to Personal Data by government authorities and shall not voluntarily cooperate with government authorities in relation to the same, and
3. no applicable law or government policy to which Importer is subject requires Importer to create or maintain backdoors or to facilitate access to Personal Data or systems or for Importer to be in possession of any corresponding encryption keys.

Access to Personal Data by government authorities

1. Importer shall notify Exporter immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data of Exporter. Such notification shall include details regarding the Data Subject concerned, Personal Data requested, the requesting authority, the legal basis for the request, and any responses provided.
2. Importer shall (i) assess the legality of the request under applicable law; (ii) exhaust all available remedies to challenge the request where there are legal grounds to do so; (iii) document such legal assessment and challenges to the request; (iv) upon request, make such documentation available to Exporter and competent Supervisory Authority. Importer shall reasonably cooperate with Exporter in relation to such request and provide Exporter with prompt updates at regular intervals with regards to any additional information related to the request. Exporter shall have the right to defend such action in lieu of and/or on behalf of Importer. Exporter may, if it so chooses, seek a protective order. Importer shall reasonably cooperate with Exporter in such defense.
3. Where Importer is prohibited from satisfying Clause 5 under applicable law, Importer shall use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. Importer agrees to document its best efforts in order to be able to demonstrate them on request of Exporter.
4. Where Importer becomes aware of any direct access by government authorities to Personal Data (including the reasonable suspicion thereof), Importer shall promptly notify Exporter with all information available to Importer, unless otherwise prohibited by applicable law.

ANNEX III TO THE STANDARD CONTRACT CLAUSES

AUTHORIZED SUBCONTRACTORS

Please see: https://www.dashlane.com/privacy/subprocessor

EXHIBIT 5 DPA
UK ADDENDUM

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the UK Information Commissioner for parties making Restricted Transfers. The UK Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Capitalized terms used in this Addendum have the meaning set out in Part 2 below.

Part 1: Tables

Table 1: Parties

Start date	As of the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: *Client as indicated on the Order Form / Agreement* Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Dashlane USA, inc. Trading name (if different): Main address (if a company registered address): 44 West 8th Street, 4th Floor, New York, NY 10011 Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): *As set forth in the Order Form / Agreemment* Job Title: Contact details including email:	Full Name (optional): Job Title: General Counsel Contact details including email: legal@dashlane.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
2	Yes	Included	N/A	Option 1: Specific Prior Authorisation.	Specified time period is fifteen (15) days.	No

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Parties as listed above

Annex 1B: Description of Transfer: *Categories of data subjects whose personal data is transferred* *Categories of personal data transferred* *Sensitive data transferred (if applicable)* *The frequency of the transfer* *Nature of the processing* *Purpose(s) of the data transfer and further processing* *The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Those in annex II above
Annex III: List of Sub processors (Modules 2 and 3 only): Those at https://www.dashlane.com/privacy/subprocessor

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms will have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    (a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    (b) Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    (c) this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    (a) References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    (b) In Clause 2, delete the words:

    "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    (c) Clause 6 (Description of the transfer(s)) is replaced with:

    "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    (d) Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

(e) Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

(f) References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

(g) References to Regulation (EU) 2018/1725 are removed;

(h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

(i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

(j) Clause 13(a) and Part C of Annex I are not used;

(k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

(l) In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

(m) Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

(n) Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

(o) The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

(a) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

(b) reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

(a) its direct costs of performing its obligations under the Addendum; and/or

(b) its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.