LastPass

DATA PROCESSING ADDENDUM

Revised: January 2025

This Data Processing Addendum ("**DPA**") supplements and forms part of the Terms of Service or other written or electronic agreement (the "**Agreement**") between LastPass and the "**Customer**" purchasing online services from LastPass (the "**Services**"). The Processor for provision of the Services is the applicable LastPass contracting entity identified at https://www.lastpass.com/legal-center/contracting-entities (referred to in this DPA as "**LastPass**"). This DPA applies to the Processing of Customer Personal Data by LastPass, including Customer Personal Data contained within Customer Content, on behalf of Customer while Customer utilizes the LastPass Services. Customer enters this DPA on behalf of itself, and to the extent required under Data Protection Laws and Regulations, on behalf of its Authorized Affiliates. As used herein, any references to the: (a) "Customer" shall hereafter include Customer and its Authorized Affiliates; (b) unless otherwise specified, "LastPass" shall hereafter include LastPass and its Affiliates; and (c) "Agreement" will be construed to include this DPA. All capitalized terms not defined herein shall have the meaning given to them in the Agreement. This DPA consists of distinct parts: the main body of the DPA, and, as applicable, Schedules 1 and 2. By executing this DPA, LastPass and Customer agree to comply with the following provisions with respect to any Customer Personal Data, each acting reasonably and in good faith.

Signature by Customer and LastPass on Page 5 of this DPA constitutes signature and acceptance of the Standard Contractual Clauses including its Appendix (as populated by the information located in this DPA and its schedules) and any permissible variations specified herein, to the extent the Standard Contractual Clauses or its variations are applicable and required for the lawful transfer and Processing of Customer Personal Data.

HOW THIS DPA APPLIES

This DPA is executed by and between the Parties. Customer's Authorized Affiliates will also be covered by this DPA, provided that Customer shall remain responsible for the acts and omissions of its Authorized Affiliates. For the avoidance of doubt, the Customer entity that is the contracting party to the Agreement shall, on behalf of itself and its Authorized Affiliates: (a) remain responsible for coordinating, making, and receiving all communication with LastPass under this DPA; and (b) exercise any of its own or its Authorized Affiliates' rights herein in a combined manner.

DATA PROCESSING TERMS

1. DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
"**Authorized Affiliate**" means any Affiliate of Customer which is (a) subject to Data Protection Laws and Regulations; and (b) authorized by Customer to use the Services pursuant to this Agreement between Customer and LastPass but has not signed its own Order Form with LastPass and is not otherwise a "Customer" under the Agreement.
"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act (CPRA), and its implementing regulations.
"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.
"**Customer Content**" means usernames, passwords, secure notes, files, documents, or similar data that Customer or its end-users upload, store, retrieve, or input (e.g., manually or via optional functionality such as password save and fill) to Customer's LastPass vault in connection with Customer or its end-users use of the Services.
"**Customer Personal Data**" means any Personal Data submitted to LastPass by or on behalf of Customer in connection with Customer's use of the Services.
"**Data Protection Laws and Regulations**" means all laws and regulations, including the laws and regulations of Brazil, the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, and the United States and its states (e.g., CCPA, Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act (CPA), etc.), in each case, to the extent applicable to the Processing of Personal Data under the Agreement.
"**Data Subject**" means the identified or identifiable person to whom Personal Data relates as defined by Data Protection Laws and Regulations including a "Consumer" as the term is defined in the CCPA.
"**Data Subject Request**" means a request from a Data Subject to exercise their privacy rights afforded to them by Data Protection Laws and Regulations. These may include the right: (i) of access; (ii) of rectification; (iii) of restriction of processing; (iv) of erasure (e.g., a "right to be forgotten"); (v) of data portability; (vi) to know any first- or third-party sharing activities; (vii) to know LastPass' relevant processing activities; (viii) to review the consequences of any objections or consent withdrawals; (ix) to not be subject to automated individual decision making; and/or (x) to object to Processing.
"**EEA**" means the European Economic Area.
"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
"**LGPD**" means Brazil Law No. 13.709, the General Law on Protection of Personal Data, as amended.
"**Party**" or "**Parties**" means either and as applicable, Customer or LastPass individually, or both entities together, respectively.
"**Personal Data**" means any information relating to: (i) an identified or identifiable natural person (e.g., a Data Subject or Consumer); and/or (ii) an identified or identifiable legal entity (e.g., a household under CCPA) where such information is protected similarly by Data

Protection Laws and Regulations.
"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including, as applicable, a "Service Provider" as the term is defined by the CCPA.
"**Technical and Organizational Measures**" or "**TOMs**" means the applicable technical and organizational measures documentation located at https://www.lastpass.com/trust-center/resources.
"**Security Incident**" means any actual breach of LastPass' security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any Customer Personal Data or Customer Content transmitted, stored or otherwise Processed by LastPass or its Sub-processors of which LastPass becomes aware.
"**Standard Contractual Clauses**" means the standard contractual clauses, also known as "SCCs," attached to the European Commission's Implementing Decision (EU) 2021/914 available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.
"**Sub-processor**" means any Processor engaged by LastPass to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.
"**Supervisory Authority**" means an independent public authority established under applicable law to oversee compliance with Data Protection Laws and Regulations.
"**Swiss FADP**" means the Swiss Federal Act on Data Protection of 19 June 1992 and its corresponding ordinances, in each case, as may be amended, superseded, or replaced.
"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under S119A Data Protection Act 2018, which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance.

2. PROCESSING OF CUSTOMER PERSONAL DATA

2.1 Roles of the Parties. The Parties agree to comply with applicable Data Protection Laws and Regulations. With regard to the Processing of Customer Personal Data by LastPass on behalf of Customer, the Parties agree that Customer is the Controller, LastPass is the Processor, and LastPass will engage Sub-processors as further detailed in Section 5 (Sub-processors) below.

2.2 Customer's Responsibilities. When using the Services, Customer shall Process Customer Personal Data in accordance with Data Protection Laws and Regulations, including maintaining lawful basis (e.g., consent), and warrants that it has all necessary rights to use and provide Customer Personal Data to LastPass. Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Laws and Regulations.

2.3 LastPass' Responsibilities. LastPass shall:

2.3.1 Treat Customer Personal Data in a confidential manner, consistent with Section 6 of this DPA;
2.3.2 Only retain, use, disclose, and Process Customer Personal Data in accordance with Customer's documented instructions, which are deemed given for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s) for the benefit of the Customer; (ii) Processing initiated by users in their use of the Services; (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement; and (iv) Processing in order to comply with applicable law, in which case LastPass agrees to promptly notify Customer of its legal obligation unless legally prohibited from doing so;
2.3.3 Immediately notify Customer if, in its opinion, any instruction is contrary to GDPR or any other Data Protection Law or Regulation;
2.3.4 Not to "sell" (as defined by CCPA) Customer Personal Data;
2.3.5 Immediately inform Customer if, in its opinion, it believes that any instructions of Customer conflict with or infringe the requirements of applicable Data Protection Laws and Regulations;
2.3.6 As required by applicable Data Protection Laws and Regulations, not combine Customer Personal Data it receives from, or on behalf of, Customer with Personal Data it receives from a third party or through its own interaction with the Data Subject; and
2.3.7 Notify Customer if, in its reasonable opinion, LastPass can no longer meet its obligations under applicable Data Protection Laws and Regulations.

2.4 Processing Details. The categories of Data Subjects, categories of Customer Personal Data transferred, sensitive data transferred (if applicable), frequency of the transfer, nature and purpose of Customer Personal Data transfer and Processing – including business purpose(s) of the Processing, retention of Customer Personal Data, and subject matter of the Processing are specified in Schedule 1 (Description of the Processing and Transfer) of this DPA.

3. RIGHTS OF DATA SUBJECTS

Unless legally prohibited from doing so, LastPass shall not respond to the request except to direct the applicable Data Subject to Customer in the event that it receives a Data Subject Request. Taking into account the nature of the Processing, LastPass shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's

obligation to respond to requests related to a Data Subject's rights under applicable Data Protection Laws and Regulations.

4. LASTPASS PERSONNEL

LastPass shall ensure that its personnel engaged in the Processing of Customer Personal Data: (a) are informed of the confidential nature of the Customer Personal Data and are bound by a duty of confidentiality; (b) have received appropriate training on their responsibilities, specifically pertaining to security and privacy measures; and (c) only have access to Customer Personal Data to the extent reasonably determined to be necessary in order to perform any obligations, responsibilities, or duties as further specified in this DPA and the Agreement. To the extent permitted by applicable law, the confidentiality obligations specified in this Section 4 shall survive the termination of the personnel engagement.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that: (a) LastPass Affiliates may be retained as Sub-processors; and (b) LastPass may engage third-party Sub-processors in connection with the provision and operation of the Services. Prior to engaging any Sub-processors (whether a third party or LastPass Affiliate), LastPass shall carry out appropriate due diligence on the Sub-processor and enter into a written agreement with each Sub-processor, which provides for sufficient guarantees from the Sub-processor to implement appropriate technical and organizational measures containing the same level of data protection obligations with respect to the protection of Customer Personal Data in such a manner that the processing will meet the requirements of applicable Data Protection Laws and Regulations.

5.2 Current Sub-processors and Notice of New Sub-processors. Customer approves the LastPass Affiliate and third-party Sub-processors found at the LastPass Trust and Privacy Center (also accessible via https://www.lastpass.com/trust-center/resources). LastPass may remove, replace, or appoint suitable and reliable further Sub-processors at their own discretion in accordance with this Section 5.2 and Section 5.3. LastPass' most up-to-date list of Sub-processors utilized for the Services and their geographic location ("**Sub-processor Disclosure**") may be found at the preceding link in this Section 5.2. LastPass shall inform Customer of any new Sub-processors by providing an updated disclosure on its Trust and Privacy Center at https://www.lastpass.com/trust-center/resources as well as via e-mail no less than fifteen (15) business days before authorizing such Sub-processors to Process Customer Personal Data in connection with the provision of the applicable Services. To enable receipt of e-mail notifications of new Sub-processors or material modifications of the Sub-processor Disclosure or Technical and Organizational Measures, Customer may subscribe here (also available at https://www.lastpass.com/trust-center/resources).

5.3 Objection Rights. Customer may, in good faith reasonably object to use by LastPass of a new Sub-processor by notifying LastPass promptly in writing (e-mail acceptable) within fifteen (15) business days after LastPass' notice in accordance with the mechanism set out in Section 5.2. Such notice shall explain Customer's good faith, reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, LastPass will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Customer Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If the Parties are unable to resolve such objection or LastPass is otherwise unwilling to resolve or make available such change within a reasonable period of time, Customer may, by providing written notice to LastPass, terminate the applicable Order Form(s) with respect to those Services which cannot be provided by LastPass without the use of the objected-to new Sub-processor. LastPass will refund Customer any prepaid, unused fees covering the remainder of the term of such Order Form(s) following the effective date of termination solely with respect to such terminated Services and will not impose any penalty for such termination.

5.4 Liability. LastPass shall be liable for the acts and omissions of its Sub-processors to the same extent LastPass would be liable if performing the applicable Sub-processor services directly under the terms of this DPA.

6. SECURITY

6.1 Protection of Customer Personal Data. Taking into account the state of the art; the costs of implementation; and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, LastPass shall implement and maintain appropriate technical and organizational measures for protection of the security (including protection against a Security Incident, as defined below), confidentiality, and integrity of Customer Personal Data, as set forth in the applicable Technical and Organizational Measures. LastPass regularly monitors compliance with these measures and will not take any action to, intentionally or negligently, materially decrease the overall security of the Services during a subscription term.

6.2 Third-Party Certifications and Audits. LastPass maintains an audit program to verify compliance with the obligations set forth in this DPA and shall make available to Customer all information necessary to demonstrate compliance with its obligations under this DPA and required by applicable Data Protection Laws and Regulations by making available, upon Customer's reasonable request and no more than once annually: (a) any written technical documentation that LastPass makes available or generally provide to its customer base; and (b) information regarding LastPass' compliance with the obligations in this DPA, in the form of applicable third-party certifications and audits, including those specified in the applicable Technical and Organizational Measures available on LastPass' Trust and Privacy Center (also accessible via https://www.lastpass.com/trust-center/resources). Where required under Data

Protection Laws and Regulations, the preceding may also include relevant information and documentation about LastPass' Sub-processors, to the extent such information is available and may be distributed by LastPass. Should additional audit activities be deemed reasonably necessary, for example if there is: (i) a requirement under Data Protection Laws and Regulations; (ii) a Security Incident; (iii) a material adverse change or reduction to the relevant data protection practices for LastPass' Services; or (iv) a breach of the material terms of this DPA, Customer may contact LastPass to request an audit by Customer directly, or by an auditor appointed by Customer, of the procedures relevant to the protection of Customer Personal Data under this DPA. Before the commencement of any such audit, Customer and LastPass shall mutually agree upon the scope, timing, duration, and reimbursable expenses (if any and solely to the extent permitted by Data Protection Laws and Regulations) of the audit. Customer shall: (a) promptly provide LastPass with information regarding any non-compliance discovered during the course of an audit; and (b) use best efforts to minimize interference with LastPass' business operations when conducting any such audit.

6.3 Data Protection Impact Assessment. If, pursuant to Data Protection Laws and Regulations, Customer is required to conduct a data protection impact assessment, prior consultation with a Supervisory Authority having appropriate jurisdiction, privacy impact assessment, or the equivalent construct in connection with their use of the Services provided by LastPass under this DPA, LastPass shall provide reasonable cooperation and assistance to Customer in helping to fulfill these obligations, to the extent such information is available to LastPass.

7. NOTIFICATIONS REGARDING CUSTOMER PERSONAL DATA

LastPass maintains security incident management policies and procedures, as further specified in the Technical and Organizational Measures, and shall notify Customer, without undue delay, but not to exceed 72 hours, after becoming aware of a Security Incident. Notification provided under this Section 7 shall not be interpreted or construed as an admission of fault or liability by LastPass. LastPass shall make reasonable efforts to identify the cause of such Security Incident and take those steps as LastPass deems necessary and reasonable in order to remediate the cause of such a Security Incident to the extent the remediation is within LastPass' reasonable control. Additionally, LastPass shall provide Customer with relevant information about the Security Incident, as reasonably required to assist Customer in ensuring Customer's compliance with its own obligations under Data Protection Laws and Regulations, such as to notify any Supervisory Authority or Data Subject in the event of a Security Incident.

8. DELETION AND RETURN OF CUSTOMER PERSONAL DATA

Following the termination or expiration of Customer's Agreement or earlier upon Customer's written request, LastPass shall delete and make irretrievable Customer Personal Data, unless European Union law, European Union or Member State law, or applicable Data Protection Laws and Regulations require or permit further storage of such Customer Personal Data. In the event LastPass is required by applicable law to retain some or all of Customer Personal Data, LastPass shall promptly notify Customer and continue to apply the same protections to the Customer Personal Data as outlined in this DPA. Data retention periods shall be in accordance with the procedures and timeframes specified in the Technical and Organizational Measures. Upon reasonable request of Customer, LastPass shall confirm in writing the deletion of Customer Personal Data. Additionally, upon Customer's written request, LastPass shall direct Customer on how to conduct a self-service data export of Customer Personal Data.

9. LIMITATION OF LIABILITY

Each Party's liability, including the liability of all of its Affiliates, arising out of or related to this DPA and all DPAs between Authorized Affiliates and LastPass, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference to the liability of a Party means the total liability of that Party and all of its Affiliates under the Agreement and all DPAs together.

10. DATA TRANSFER

10.1 If, during performance of the Services, Customer Personal Data that is subject to GDPR, LGPD, or any other Data Protection Law or Regulation is transferred to a jurisdiction for processing which is deemed to be a third country without an adequate level of data protection within the meaning of Data Protection Laws and Regulations, the transfer mechanism(s) provided below shall apply to such transfers:

10.1.1 The Standard Contractual Clauses shall apply in addition to this DPA. The Standard Contractual Clauses shall be structured as follows: (i) Module Two (Controller to Processor) terms shall apply and Modules One, Three, and Four shall be deleted in their entirety; (ii) Clause 7 shall be deleted in its entirety and the Parties may add additional entities to this DPA by executing an additional DPA, as made available at https://www.lastpass.com/legal-center; (iii) in Clause 9, Option 2 shall apply (as detailed in Section 5 of this DPA); (iv) in Clause 11, the optional independent dispute resolution body that LastPass makes available to Data Subjects at no cost is provided through TrustArc, a third-party privacy firm, at https://feedback-form.truste.com/watchdog/request; (v) in Clause 17, Option 1 shall apply and the Standard Contractual Clauses shall be governed by the Republic of Ireland; (vi) in Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland; and (vii) the Annexes of the Standard Contractual Clauses shall be populated with the information set out in the Schedules to this DPA.

10.1.2 For Customers and Data Subjects who are residents of the United Kingdom, LastPass shall, where applicable: (a) provide its Services in accordance with its obligations under the UK Addendum, which is incorporated into this DPA by reference; and (b) as required by applicable law, transfer and process Customer Personal Data on the basis of the Standard Contractual Clauses, as modified in accordance with the UK Addendum. The UK Addendum shall be structured as follows: (i) Table 1 shall be populated by the information in Schedule 2 of the DPA; (ii) Table 2 shall be populated by the information in Section 10.1.1 of the DPA with the exception that the IDTA will be governed by England and Wales; (iii) Table 3 shall be populated by Schedules 1 and 2 of the DPA; and (iv) in Table 4, either the Importer or the Exporter may terminate this Addendum.

10.1.3 For Customers and Data Subjects who are residents of Switzerland, LastPass shall, as required by applicable law, protect, transfer, and process Customer Personal Data on the basis of the Standard Contractual Clauses, which are incorporated into this DPA by reference. Where this section applies, the Standard Contractual Clauses shall be modified as follows: (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss FADP; (ii) references to "EU," "Union," and "Member State" shall be amended to include Switzerland; (iii) references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the "Swiss Federal Data Protection and Information Commissioner" and the "competent Swiss courts"; (iv) the term "member state" as used in Standard Contractual Clauses shall not be interpreted to exclude Data Subjects in Switzerland from exercising applicable rights (e.g., in their habitual place of residence); (v) the Standard Contractual Clauses shall be governed by the laws of Switzerland and disputes shall be resolved before the Swiss courts having appropriate jurisdiction.

10.1.4 The Standard Contractual Clauses will not apply to the data transfer if LastPass adopts an alternative, recognized compliance standard for lawful data transfers, such as the EU-US Data Privacy Framework.

10.2 LastPass shall promptly notify the Customer of any transfers of Customer Personal Data to a third country without an adequate level of protection as required by Data Protection Laws and Regulations before initiating the Processing.

10.3 To the extent that the Parties are relying on a specific statutory mechanism to normalize international data transfers and that mechanism is subsequently modified, revoked, or held in a court with applicable authority to be invalid, the Parties agree to cooperate in good faith to pursue an alternative mechanism (if available and required) to permit the continued transfer of Customer Personal Data.

11. PRIVACY CERTIFICATIONS

LastPass maintains certain certifications which are available at the LastPass Trust and Privacy Center at https://www.lastpass.com/trust-center. LastPass participates in APEC CBPR system and shall Process Customer Personal Data, where applicable, in accordance with the obligations and responsibilities of a Processor under those certifications.

12. LEGAL EFFECT AND CONFLICT

This DPA shall become legally binding between Customer and LastPass upon execution of the Agreement. Once effective, this DPA shall be incorporated into and form part of the Agreement or applicable Order Form. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the Parties vis-à-vis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will control.

List of Schedules:
Schedule 1: Description of the Processing and Transfer
Schedule 2: Provisions Related to the Standard Contractual Clauses

The Parties' authorized signatories have duly executed this Agreement:

Customer:	**On behalf of LastPass**: [*In its own name and on behalf of each LastPass contracting entity*]
By: _____	By: _____
Name:	Name:
Title:	Title:
Effective Date:	

SCHEDULE 1 - DESCRIPTION OF THE PROCESSING AND TRANSFER

Categories of Data Subjects

Customer may submit Customer Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Customer Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's users (who are natural persons) authorized by Customer to use the Services

Categories of Personal Data Transferred

Customer may submit Customer Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Customer Personal Data:

- First and last name
- Title
- Employer
- Contact information (company, email, phone, physical business address)
- Device identification data and usage data (e.g., MAC addresses, web logs, etc.)
- Localisation data
- Credentials and Customer Content (encrypted using our zero-knowledge security model)

Sensitive Data Transferred (If Applicable)

The Parties do not anticipate that any sensitive data will be transferred. However, it is possible for Customer to choose to submit sensitive data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and for which relevant safeguards are specified in the Technical and Organizational Measures documentation herein.

Frequency of the Transfer

The frequency, type, nature, and purpose of the data transfer will be dependent upon Customer's individual use case (i.e., transfer frequency may be continuous and/or may be limited in time to a specific session or event).

Nature and Purpose of Personal Data Transfer and Processing

LastPass will Process and transfer Customer Personal Data, in its capacity as a Processor, and engage Sub-processors, as necessary to perform and operate the Services pursuant to the Agreement, as further specified in the applicable Sub-Processor Disclosure (Section 5 of this DPA) and Technical and Organizational Measures documentation, and to the extent further instructed by Customer through its use of the Services.

Retention of Personal Data

LastPass will Process and retain Customer Personal Data, in its capacity as a Processor, for the duration of the Agreement (as further specified in the Technical and Organizational Measures), unless otherwise agreed upon in writing.

Subject-Matter of the Processing

LastPass provides, directly and through its Sub-processors, identity and access management solutions. The objective and subject of the Processing of Customer Personal Data by LastPass, as a Processor, is servicing Customer and providing, supporting, and operating the provision of the Services.

SCHEDULE 2 – PROVISIONS RELATED TO THE STANDARD CONTRACTUAL CLAUSES

Identified Parties and Competent Supervisory Authority

Data Exporter

Name: Customer and its Authorized Affiliates established within the European Economic Area and/or Switzerland.

Address: The Customer address identified on the relevant order documentation or Order Form, as applicable.

Contact Person's Name, Position, and Contact Details: Customer's primary contact, position, and details as identified on the relevant order documentation or Order Form, as applicable.

Activities Relevant to the Data Transferred Under the Standard Contractual Clauses: Customer (data exporter) procures LastPass (data importer) Services in the fields of identity and access management.

Role: Data Controller

Competent Supervisory Authority: The supervisory authority of the EEA Member State in which Customer is established or, if Customer is not established in the EEA, the EEA Member State in which Customer's representative is established or in which Customer's end-users or customers are predominantly located.

Data Importer

Name: The name of the specific LastPass importing organization shall be as follows:

Country	LastPass Entity (as applicable)
United States	LastPass US LP
Ireland (outside of the EEA and EU)	LastPass Ireland Limited

Address: please see https://www.lastpass.com/legal-center/contracting-entities.

Contact Person's Name, Position and Contact Details: LastPass Privacy Team, e-mail: privacy@lastpass.com

Activities Relevant to the Data Transferred Under the Standard Contractual Clauses: LastPass provides a password management solution that allows users to generate, store, and share credentials for online applications and websites. The activities relevant to and/or the objective and subject of the Processing of Customer Personal Data by LastPass, as a Processor, is servicing Customer and providing, supporting, and operating the provision of the Services.

Role: Data Processor