Data Processing Addendum

In order that you as a service user and data controller (referred to as "Controller" or "you" or "Client") may use or continue to use the password manager services (the "Services") offered by us, Rabbit Company LLC of 1603 Capitol Avenue, Suite 413A, Cheyenne, WY, Laramie, 82001, United States and data processor (referred to as "Passky" or "Processor"), you have agreed that these data processing terms ("Terms") shall apply (notwithstanding any other terms and conditions applicable to the delivery of the Services to the contrary) in order to address the compliance obligations imposed upon Passky and its Clients pursuant to applicable Data Protection Law and in particular, Regulation (EU) 2016/679 ("GDPR").

These Terms shall constitute a separate agreement, or they may be incorporated by reference in the relevant Services agreement, as the case may be.

1. Definitions

1.1. In this Agreement, capitalised words shall have the meaning as set out below or, as the case may be, elsewhere in this Agreement:

1.1.1. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with, a party from time to time during the Term.

1.1.2. "Data Protection Law" means the data privacy laws applicable to the processing in connection with the Services, including, where applicable, the GDPR or similar law, or the applicable data privacy laws of any other relevant jurisdiction.

1.1.3. "Client" means any client of Passky.

1.1.4. "Contractual Clauses" means the standard contractual clauses of the European Commission for the transfer of personal data across borders, as amended or replaced from time to time, or any equivalent set of contractual clauses approved for use under Data Protection Law; and

1.1.5. "Personal Data" means the personal data processed by Processor in connection with the Services on behalf of Client during the Term and may include Personal Data, and Special Categories Data as specifically required and transferred by the Client. The processing may include activities auxiliary to Passky services, such as administrative and other services. This will include names and other information about data subjects included in Client materials.

1.1.6. The words "data subject", "personal data", "processing" and variations, "controller" and "processor" shall have the meaning attributed to them in Data Protection Law.

2. Appointment

2.1. Passky is designated by its Clients, Client Affiliates and Business Affiliates (collectively "Instructing Parties") to provide and manage various services, including the Services on their behalf. Accordingly, Personal Data may contain personal data in relation to which Client and its Instructing Parties are controllers. Passky confirms that it is authorised to communicate to Client any instructions or other requirements on behalf of Client in respect of processing of Personal Data connection with the Services.

2.2. Processor is appointed by Client to process Personal Data on behalf of Client and/or the Instructing Parties, as the case may be, as is necessary to provide the Services or as otherwise agreed by the parties in writing.

3. Duration

The Terms shall commence on the Effective Date and shall continue in full force and effect until such time as all Services have ceased and all Personal Data in the Processor's possession or within its reasonable control has been returned or destroyed (the "Term").

4. Data Protection Compliance

4.1. In relation to its processing of Personal Data, save as otherwise required by law, Passky agrees to:

4.1.1. process Personal Data only as required in connection with the Services and in accordance with Client and its Instructing Parties documented lawful instructions from time to time;

4.1.2. inform Client and its Instructing Parties if, in Passky`s opinion, an instruction infringes Data Protection Law;

4.1.3. ensure that all personnel authorised by Passky to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

4.1.4. implement appropriate technical and organisational measures to appropriately safeguard Personal Data having regard to the nature of the personal data which is to be protected and the risk of harm which might result from any Security Breach (as defined below), at a minimum the measures set out in the Schedule;

4.1.5. promptly inform Client and its Instructing Parties of any data subject requests under Data Protection Law or regulatory or law enforcement requests relating to Personal Data. Passky shall not acknowledge or otherwise respond to the subject access request except with Client and its Instructing Parties prior written approval, which shall not be unreasonably withheld;

4.1.6. provide such assistance as Client and its Instructing Parties may reasonably require in order to ensure Passky's compliance with Data Protection Law in relation to data security, data breach notifications, data protection impact assessments and prior consultations with a competent authority;

4.1.7. at Client and its Instructing Parties choice, without delay delete or return all Personal Data to Client and its Instructing Parties, and delete existing copies of all Personal Data in the Processor's possession or within its reasonable control (including those held by a Sub processor); and

4.1.8. make available to Client and its Instructing Parties information reasonably necessary to demonstrate Passky compliance with these Terms and allow for, and contribute to, audits and inspections carried out by Client and its Instructing Parties.

5. Sub processors

5.1. Processor will sub-contract, outsource, assign, novate or otherwise transfer obligations under these Terms or engage any subcontractors involved in the processing of Personal Data (each a “Sub processor”) only with Client's prior written consent and subject to subclause 5.2.

5.2. When engaging a Sub processor, Processor will:

5.2.1. carry out reasonable due diligence;

5.2.2. enter into a contract on terms, as far as practicable, same as those in these Terms, and which may include Contractual Clauses to provide adequate safeguards with respect to the processing of Personal Data; and

5.2.3. inform Client of any intended changes concerning the addition or replacement of a Sub processor from time to time. If Client object`s to any such change on reasonable grounds, then acting in good faith the parties will work together to resolve such objection.

6. Security Incidents

6.1. “Security Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

6.2. Processor will investigate the Security Breach and take reasonable action to identify, prevent and mitigate the effects of the Security Breach. Processor will take such further action as Client may reasonably request in order to comply with Data Protection Law.

6.3. Processor may not release or publish any filing, communication, notice, press release, or report concerning any Security Breach (“Notices“) without Client`s prior written approval; such approval shall not be unreasonably withheld.

6.4. Passky will notify Client without undue delay if Passky becomes aware of any Security Breach within 24 hours of discovering such Breach and provide Client with:

6.4.1. a detailed description of the Security Incident;

6.4.2. the type of data that was the subject of the Security Incident;

6.4.3. the identity of each affected person, and

6.4.4. the steps Passky takes in order to mitigate and remediate such Security Incident, in each case as soon as such information can be collected or otherwise becomes available.

6.5. Passky shall use its best efforts to immediately mitigate and remedy any Security Incident and prevent any further Security Incident(s) at its sole expense.

6.6. Passky agrees that Client shall have the sole right to determine (i) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Client's discretion, (ii) the contents of such notice, and (iii) whether any type of remediation may be offered to affected persons, as well as the nature and extent of any such remediation.

6.7. In the event of a Security Incident involving Personal Data in Passky's possession or otherwise caused by or related to Passky's acts or omissions, and without limiting Client's other rights and remedies, Passky will pay all costs and expenses of (i) any disclosures and notification required by applicable law or as otherwise determined as appropriate in Client's reasonable discretion, (ii) monitoring and reporting on the impacted individuals' or entities' credit records if determined in Client's reasonable discretion as reasonable to protect such individuals, and (iii) all other costs incurred by Client in responding to, remediating and mitigating damages caused by such Security Incident.

6.8. Passky will investigate the Security Breach and take reasonable action to identify, prevent and mitigate the effects of the Security Breach. Passky will take such further action as Client may reasonably request in order to comply with Data Protection Law.

6.9. Passky may not release or publish any filing, communication, notice, press release, or report concerning any Security Breach ("Notices") without Client`s prior written approval; such approval shall not be unreasonably withheld.

7. Audit

7.1. Client (or its designated representatives) may, on an annual basis or more frequently as reasonably requested by Client, at Client's expense, conduct an audit to verify that Passky is operating in accordance with this DPA. Such audit(s) may include a review of all aspects of Passky's performance, including, but not limited to, Passky's general controls and security practices and procedures. Passky will cooperate with Client in conducting any such audit, and will allow Client reasonable access, during normal business hours and upon reasonable notice, to all pertinent records, documentation, computer systems, data, personnel and areas used to Process the Client Data areas as Client reasonably requests to complete such audit. Client will take reasonable steps to prevent the audit from materially impacting Passky's operations.

7.2. Passky shall correct any deviations from Security Best Practices that are identified in any security audit as soon as practicable, but in no event more than five days after receiving notice from Client outlining any deviations (provided, however, that if five days is not a practicable cure period, then Passky may instead present a remediation plan to Client within such five day period that sets forth an achievable and reasonable timeframe, and Passky must thereafter diligently proceed to correct any deviations in accordance with such plan).

8. International Data Transfers

8.1. Passky will ensure that no Personal Data are transferred out of either:

8.1.1. the by the Client approved data environment; or

8.1.2. any territory in which restrictions are imposed on the transfer of Personal Data across borders under Data Protection Laws,

8.1.3. without the prior written consent of Client.

8.1.4. Passky will ensure that Contractual Clauses or other applicable transfer mechanism, are in place to ensure adequate level of data protection.

9. Indemnity

Notwithstanding any provisions of the relevant Services agreement to the contrary, Processor shall and hereby agrees to indemnify Client and Instructing Parties and their officers, employees, agents and subcontractors (each an "Indemnified Party") from and against any claims, losses, demands, actions, liabilities, fines, penalties, reasonable expenses, damages and settlement amounts (including reasonable legal fees and costs) incurred by any Indemnified Party as a result of any gross negligence or wilful breach by Processor of these Terms.

10. Miscellaneous

10.1. Clause and other headings in these Terms are for convenience only and shall not affect the meaning or interpretation of these Terms.

10.2. To the extent of any conflict, these Terms shall prevail over any Services agreement or other agreement.

10.3. Nothing in these Terms will exclude or limit the liability of either party which cannot be limited or excluded by applicable law. Subject to the foregoing sentence, (i) these Terms, including any appendices, constitutes the entire agreement between the parties pertaining to the subject matter hereof and supersedes all prior agreements, understandings, negotiations and discussions of the parties relating to its subject matter; and (ii) in relation to the subject matter of these Terms neither party has relied on, and neither party will have any right or remedy based on, any statement, representation or warranty, whether made negligently or innocently, except those expressly set out in these Terms.

10.4. Client shall agree any amendment to these Terms that may be required from time to time for us and Instructing Parties to comply with any amended Data Protection Laws.

10.5. All notices of termination or breach must be in English, in writing and addressed to the other party's primary contact person or legal department. Notice will be treated as given on receipt, as verified by a valid receipt or electronic log. Postal notices will be deemed received 48 hours from the date of posting by recorded delivery or registered post.

10.6. The provisions of these Terms are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of these Terms shall remain in full force and effect.

10.7. These Terms are governed by the law of Wyoming and the parties submit to the exclusive jurisdiction of the courts of Wyoming in relation to any dispute (contractual or non-contractual) concerning these Terms save that either party may apply to any court for an injunction or other relief to protect its property or confidential information.

11. SCHEDULE

11.1. Security measures

11.1.1. Passky represents, warrants, and undertakes that it has established and for so long as Passky Processes Personal Data it will at all times enforce, an ongoing program of Security Policies, Security Procedures, and Security Technical Controls, which reasonably ensures delivery of Security Best Practices, and which includes, without limitation, the following:

11.2. Information Security

11.2.1. a privacy and security incident management program;

11.2.2. a privacy and security awareness program;

11.2.3. business continuity and disaster recovery plans, including regular testing; and

11.2.4. procedures to conduct periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for timely and appropriate remediation.

11.3. **Physical Access**

11.3.1. physical protection mechanisms for all information assets and information technology to ensure such assets and technology are stored and appropriately protected;

11.3.2. appropriate facility and room entry controls to limit physical access to systems that store or process Client Data;

11.3.3. processes to ensure access to facilities and rooms are monitored and is restricted on a "need to know" basis; and

11.3.4. controls to physically secure all Client Data and to securely destroy such information when it is no longer needed in accordance with this Agreement.

11.4. **Logical Access**

11.4.1. appropriate mechanisms for user authentication and authorisation in accordance with a "need to know" policy;

11.4.2. controls and auditable logs to enforce and maintain rigorous access restrictions for employees, and subcontractors;

11.4.3. timely and accurate administration of user account and authentication management;

11.4.4. processes to ensure Passky-supplied defaults for passwords and security parameters are appropriately managed (e.g., changed periodically etc.);

11.4.5. mechanisms to encrypt or hash all passwords or otherwise ensure all passwords are not stored unsecured in clear text; and

11.4.6. processes to immediately revoke accesses of inactive accounts or terminated/transferred users.

11.5. **Security Architecture and Design**

11.5.1. a security architecture that reasonably ensures delivery of Security Best Practices;

11.5.2. documented and enforced technology configuration standards;

11.5.3. regular testing of security systems and Security Best Practices;

11.5.4. a system of effective firewall(s) and intrusion detection technologies necessary to protect Client Data; and

11.5.5. database and application layer design processes that ensure web applications are designed to protect the information data that is Processed through such systems.

11.6. **System and Network Management**

11.6.1. mechanisms to keep security patches current;

11.6.2. monitor, analyse, and respond to security alerts;

11.6.3. appropriate network security design elements that provide for segregation of data from other third-party data;

11.6.4. use and regularly update anti-virus software; and

11.6.5. the integrity, resilience and availability of any software or services utilised to Process the Client Data.

11.6.6. Failure by Passky to comply with Security Best Practices or its obligations hereunder shall constitute a breach of the Agreement.

11.7. **Minimum technical measures**

11.7.1. Firewalls which are properly configured and using the latest software;

11.7.2. user access control management;

11.7.3. unique passwords of sufficient complexity and regular expiry on all devices;

11.7.4. secure configuration on all devices;

11.7.5. regular software updates, if appropriate, by using patch management software;

11.7.6. timely decommissioning and secure wiping (that renders data unrecoverable) of old software and hardware;

11.7.7. real-time protection anti-virus, anti-malware and anti-spyware software;

11.7.8. https;

11.7.9. encryption of all portable devices ensuring appropriate protection of the key;

11.7.10.encryption of personal data in transit by using suitable encryption solutions;

11.7.11.multi-factor authentication for remote access;

11.7.12.WPA-TKIP secured WiFi access;

11.7.13.delinquent web filtering and other appropriate internet access restrictions;

11.7.14.intrusion detection and prevention systems;

11.7.15.appropriate and proportionate monitoring of personnel; and

11.7.16.data backup and disaster recovery measures and procedures.

11.7.17.Minimal organisational measures

11.7.18.Vet all personnel including staff, contractors, vendors and suppliers (including Sub processors) on continuous basis;

11.7.19.non-disclosure agreements used with all personnel;

11.7.20.regular training of all personnel on confidentiality, data processing obligations, identification of Security Breaches and risks;

11.7.21.apply principle of least authority, including a restricted or strictly controlled transit of data and material outside of office;

11.7.22.physical security on premises including reception or front desk, security passes, clean desk policy, storage of documents in secure cabinets, secure disposal of materials, etc.;

11.7.23.apply appropriate policies, as appropriate.

12. Cross Border Data Transfer Mechanisms

12.1. In the event the Services are covered by more than one Transfer Mechanism, the transfer of personal data will be subject to a single Transfer Mechanism in accordance with the following order of precedence:

12.2. Passky's binding corporate rules as set forth in this Schedule

12.3. the applicable Standard Contractual Clauses as set forth in this Schedule

12.4. other applicable data Transfer Mechanisms permitted under Applicable Data Protection Law.

13. Binding Corporate Rules

13.1. The parties agree that Passky will process personal data within the Passky Services in accordance with the data protection policies that are approved by European data protection authorities after significant consultation with those authorities and enable multinational businesses, such as Passky, to make intra-organisational transfers of personal data across borders in compliance with EU data protection law.

13.2. The parties further agree that, with respect to the Passky Services, the Binding Corporate Rules will be the lawful Transfer Mechanism of Client Account Data, Client Content, and Client Usage Data from the EEA, Switzerland, or the United Kingdom to Passky in the United States.

14. Standard Contractual Clauses

14.1. The parties agree that the 2021 Standard contractual clauses for international transfers as publish and available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en will apply to personal data that is transferred via the Services from the UK, European Economic Area or Switzerland, either directly or via onward transfer, to any country or recipient outside the UK, European Economic Area or Switzerland that is:

14.1.1. not recognised by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for personal data and

14.1.2. not covered by the above Binding Corporate Rules. For data transfers from the European Economic Area that are subject to the 2021 Standard Contractual Clauses, the 2021 Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

14.1.2.1. Module One (Controller to Controller) of the 2021 Standard Contractual Clauses will apply where Passky is processing Client Account Data and

14.1.2.2. Client is a controller of Client Usage Data and Passky is processing Client Usage Data.

14.1.2.3. Module Two (Controller to Processor) of the 2021 Standard Contractual Clauses will apply where Client is a controller of Client Content and Passky is processing Client Content.

14.1.2.4. Module Three (Processor to Processor) of the 2021 Standard Contractual Clauses will apply where Client is a processor of Client Content and Passky is processing Client Content.

14.1.2.5. Module Four (Processor to Controller) of the 2021 Standard Contractual Clauses will apply where Client is a processor of Client Usage Data and Passky processes Client Usage Data.

14.1.3. For each Module, where applicable:

14.1.3.1. Data Exporter: Client.

14.1.3.2. Contact details: The email address(es) designated by Client in Client's account via its notification preferences.

14.1.3.3. Data Exporter Role: The Data Exporter's role is set forth in this Agreement.

14.1.3.4. Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.

14.1.3.5. Data Importer: Passky.

14.1.3.6. Contact details: Passky Support Team - info@passky.org

14.1.3.7. Data Importer Role: The Data Importer's role is set forth in this Agreement.

14.1.3.8. Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

14.2. The categories of data subjects are described in this Agreement

14.3. The Sensitive Data transferred is described in this Agreement.

14.4. The frequency of the transfer is a continuous basis for the duration of the Agreement.

14.5. The nature of the processing is described in this Agreement.

14.6. The purpose of the processing is described in this Agreement.

14.7. The period for which the personal data will be retained is this Agreement.

14.8. The Supervisory Authority shall be the Information Commissioner of the Republic of Slovenia.

14.9. For transfers to sub-processors, the subject matter, nature, and duration of the processing is set forth below.

14.10. The Schedule Security Measures of this Agreement serves as Annex of the Standard Contractual Clauses.

14.11. Conflict. To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this Agreement, or the Privacy Policy, the provisions of the Standard Contractual Clauses will prevail.