



Password Boss Reseller Data Processing Addendum

This Data Processing Addendum (“DPA”) forms part of the Password Boss Non-Exclusive Reseller Agreement (or other such titled written or electronic agreement addressing the same subject matter) between Password Boss and Company for the purchase of Solutions from Password Boss (identified collectively either as the “Service”, “Solution”, or otherwise in the applicable agreement, and hereinafter defined as the “Service”), wherein such agreement is hereinafter defined as the “Agreement,” and whereby this DPA reflects the parties’ agreement with regard to the Processing of Personal Data.

Company enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Password Boss processes Personal Data for which such Authorized Affiliates qualify as the Controller. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In providing the Service to Company pursuant to the Agreement, Password Boss may Process Personal Data on behalf of Company, and the parties agree to comply with the following provisions with respect to any Personal Data.

INSTRUCTIONS ON HOW TO EXECUTE THIS DPA WITH PASSWORD BOSS

1. This DPA consists of distinct parts: this body and its set of definitions and provisions, the Standard Contractual Clauses, and Appendices 1-3.
2. This DPA has been pre-signed on behalf of PasswordBoss, LLC, as the data importer.
3. To complete this DPA, Company must: (a) Complete the information in the signature box and sign on Page 8. (b) Complete the information as the data exporter on Page 9. (c) Complete the information in the signature box and sign on Pages 17, 19, 20 and 21.
4. Company must send the completed and signed DPA to Password Boss by email to privacy@passwordboss.com, or Company may electronically sign this DPA using a link provided by Password Boss. Upon receipt of the validly-completed DPA by Password Boss at this email address, or via an electronic signature link provided by Password Boss, this DPA shall come into effect and legally bind the parties.

APPLICATION OF THIS DPA

If the Company entity signing this DPA is a party to the Agreement, then this DPA is an addendum to, and forms part of, the Agreement. In such case, the Password Boss entity (i.e., either PasswordBoss, LLC or a subsidiary of PasswordBoss, LLC) that is party to the Agreement is party to this DPA.

If the Company entity signing this DPA is neither a party to an Order nor the Agreement, then this DPA is not valid and therefore is not legally binding. Such entity should request that the Company entity who is a party to the Agreement executes this DPA.

DPA DEFINITIONS

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the Company entity signing this Agreement. “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 of Company's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Service pursuant to the Agreement between Company and Password Boss, but has not signed its own Order with Password Boss and is not a "Company" as defined under the Agreement.

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

“Company Data” means all electronic data submitted by or on behalf of Company, or an Authorized Affiliate, to the Service.

“Data Protection Laws and Regulations” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area (“EEA”) and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.

“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).

“Personal Data” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Company Data.

“Processing” (including its root word, “Process”) 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.

“Trust & Compliance Documentation” means the Documentation applicable to the specific Service purchased by Company, as may be updated periodically, and accessible via Password Boss’s website at www.passwordboss.com/agreements, or as otherwise made reasonably available by Password Boss.

“Password Boss” means the Password Boss entity which is a party to this DPA, as specified in the section “Application of this DPA” above, being PasswordBoss, LLC, a company incorporated in Minnesota and its primary address as 2751 Hennepin Ave S #252, Minneapolis, MN 55408, USA, or an Affiliate of Password Boss, as applicable.

“Password Boss Group” means Password Boss and its Affiliates engaged in the Processing of Personal Data.

“Standard Contractual Clauses” means the agreement executed by and between Company and Password Boss and included herein, pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

“Sub-processor” means any Processor engaged by Password Boss or a member of the Password Boss Group.

“Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to the GDPR.

DPA TERMS

Password Boss and the signatory below at the address below (“Company”) hereby enter into this DPA effective as of the last signature date below. This DPA is incorporated into and forms part of the Agreement.

1. **Provision of the Service.** Password Boss provides the Service to Company under the Agreement. In connection with the Service, the parties anticipate that Password Boss may Process Company Data that contains Personal Data relating to Data Subjects.
2. **The Parties’ Roles.** The parties agree that with regard to the Processing of Personal Data, Company is the Controller, Password Boss is the Processor, and that Password Boss or members of the Password Boss Group will engage Sub-processors pursuant to the requirements of this DPA.
3. **Company Responsibilities.** Company shall, in its use of the Service, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Company’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Company shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Company acquired Personal Data.
4. **Processing Purposes.** Password Boss shall keep Personal Data confidential and shall only Process Personal Data on behalf of and in accordance with Company’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order(s); (ii) Processing initiated by Users in their use of the Service; and (iii) Processing to comply with other documented, reasonable instructions provided by Company (for example, via email) where such instructions are consistent with the terms of the Agreement. Password Boss shall not be required to comply with or observe Company’s instructions if such instructions would violate the GDPR or other EU law or EU member state data protection provisions.
5. **Scope of Processing.** The subject-matter of Processing of Personal Data by Password Boss is the performance of the Service pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Appendix 1 to this DPA.
6. **Data Subject Requests.** To the extent legally permitted, Password Boss shall promptly notify Company if Password Boss receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or its right not to be subject to an automated individual decision making (“Data Subject Request”). Factoring into account the nature of the Processing, Password Boss shall assist Company by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Company’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Company, in its use of the Service, does not have the ability to address a Data Subject Request, Password Boss shall, upon Company’s request, provide commercially-reasonable efforts to assist Company in responding to such Data Subject Request, to the extent that Password Boss is legally authorized to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Company shall be responsible for any costs arising from Password Boss’s provision of such assistance.
7. **Password Boss Personnel.** Password Boss shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training regarding their responsibilities, and have executed written confidentiality agreements. Password Boss shall take commercially-reasonable steps to ensure the reliability of any Password Boss personnel engaged in the Processing of Personal Data.

Password Boss shall ensure that Password Boss's access to Personal Data is limited to those personnel assisting in the provision of the Service in accordance with the Agreement.

8. Data Protection Officer. Effective from 25 May 2018, Password Boss shall have appointed, or shall appoint, a data protection officer if and whereby such appointment is required by Data Protection Laws and Regulations. Any such appointed person may be reached at privacy@passwordboss.com.

9. Password Boss's Sub-processors. Company has instructed or authorized the use of Sub-processors to assist Password Boss with respect to the performance of Password Boss's obligations under the Agreement and Password Boss agrees to be responsible for the acts or omissions of such Sub-processors to the same extent as Password Boss would be liable if performing the services of the Sub-processors under the terms of the Agreement. Upon written request of the Company, Password Boss will provide to Company a list of its then-current Sub-processors. Company acknowledges and agrees that (a) Password Boss's Affiliates may be retained as Sub-processors; and (b) Password Boss and Password Boss's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Service. On Password Boss's Agreements webpage (accessible via www.passwordboss.com/agreements under the "Trust & Compliance Documentation" link), Company may find a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, to which Company shall subscribe, and if Company subscribes, Password Boss shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to process Personal Data in connection with the provision of the applicable Service. In order to exercise its right to object to Password Boss's use of a new Sub-processor, Company shall notify Password Boss promptly in writing within ten (10) business days after receipt of Password Boss's notice in accordance with the mechanism set out above. In the event Company objects to a new Sub-processor, and that objection is not unreasonable, Password Boss will use reasonable efforts to make available to Company a change in the Service or recommend a commercially-reasonable change to Company's configuration or use of the Service to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Company. If Password Boss is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Company may terminate the applicable Order(s) with respect only to those aspects of the Service which cannot be provided by Password Boss without the use of the objected-to new Sub-processor by providing written notice to Password Boss. Password Boss will refund Company any prepaid fees covering the remainder of the term of such Order(s) following the effective date of termination with respect to such terminated Service. The parties agree that the copies of the Sub-processor agreements that must be provided by Password Boss to Company pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Password Boss beforehand; and, that such copies will be provided by Password Boss, in a manner to be determined in its discretion, only upon request by Company.

10. Liability for Sub-processors. Password Boss shall be liable for the acts and omissions of its Sub-processors to the same extent Password Boss would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

11. Security Measures. Password Boss shall maintain appropriate organizational and technical measures for protection of the security (including protection against unauthorized or unlawful Processing, and against unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Company Data), confidentiality, and integrity of Company Data, as set forth in Password Boss's applicable Trust & Compliance Documentation. Password Boss regularly monitors compliance with these measures. Password Boss will not materially decrease the overall security of the Service during Company's and/or Authorized Affiliates' subscription term.

13. Notifications Regarding Company Data. Password Boss has in place reasonable and appropriate security incident management policies and procedures, as specified in the Trust & Compliance Documentation and shall notify Company without undue delay after becoming aware of the unlawful or accidental destruction, alteration or damage

or loss, unauthorized disclosure of, or access to, Company Data, including Personal Data, transmitted, stored or otherwise Processed by Password Boss or its Sub-processors of which Password Boss becomes aware (hereinafter, a "Company Data Incident"), as required to assist the Company in ensuring compliance with its obligations to notify the Supervisory Authority in the event of Personal Data breach. Password Boss shall make reasonable efforts to identify the cause of such Company Data Incident and take those steps as Password Boss deems necessary and reasonable in order to remediate the cause of such a Company Data Incident, to the extent that the remediation is within Password Boss's reasonable control. The obligations set forth herein shall not apply to incidents that are caused by either Company or Company's Users.

14. Return of Company Data. Password Boss shall return Company Data to Company and, to the extent allowed by applicable law, delete Company Data in accordance with the procedures and time periods specified in the Trust & Compliance Documentation, unless the retention of the data is requested from Password Boss according to mandatory statutory laws.

15. Authorized Affiliates. The parties agree that, by executing the DPA, the Company enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between Password Boss and each such Authorized Affiliate, subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. An Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Service by Authorized Affiliate(s) must comply with the terms and conditions of the Agreement and any violation thereof by an Authorized Affiliate shall be deemed a violation by Company.

16. Communications. The Company that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Password Boss under this DPA, and shall be entitled to transmit and receive any communication in relation to this DPA on behalf of its Authorized Affiliate(s).

17. Exercise of Rights. Where an Authorized Affiliate becomes a party to the DPA, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Password Boss directly by itself, the parties agree that (i) solely the Company that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Company that is the contracting party to the Agreement shall exercise any such rights under this DPA in a combined manner for all of its Authorized Affiliates together, instead of doing so separately for each Authorized Affiliate.

19. Liability. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Password Boss, 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 in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. Password Boss's and its Affiliates' total liability for all claims from the Company and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Company and all Authorized Affiliates, and shall not be understood to apply individually and severally to Company and/or to any Authorized Affiliate that is a contractual party to any such DPA. Each reference to the DPA herein means this DPA including its Appendices.

20. GDPR. Effective from 25 May 2018, Password Boss will Process Personal Data in accordance with the GDPR requirements directly applicable to Password Boss's provision of the Service.

21. Data Protection Impact Assessment. Effective from 25 May 2018, upon Company's request, Password Boss shall provide Company with reasonable cooperation and assistance needed to fulfil Company's obligation under the GDPR

to carry out a data protection impact assessment related to Company's use of the Service, to the extent Company does not otherwise have access to the relevant information, and to the extent such information is available to Password Boss. Password Boss shall provide reasonable assistance to Company in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 21 of this DPA, to the extent required under the GDPR.

22. Standard Contractual Clauses. The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Company established within the European Economic Area, Switzerland and the United Kingdom, which have submitted Orders for the Service. For the purpose of the Standard Contractual Clauses the aforementioned entities shall be deemed "data exporters."

23. Company's Processing Instructions. This DPA and the Agreement are Company's complete and final instructions at the time of signature of the Agreement to Password Boss for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Company to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order(s); (b) Processing initiated by Users in their use of the Service and (c) Processing to comply with other reasonable instructions provided by Company (e.g., via email) where such instructions are consistent with the terms of the Agreement.

24. Audits. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: following Company's written request, and subject to the confidentiality obligations set forth in the Agreement, Password Boss shall make available to Company information regarding the Password Boss Group's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Trust & Compliance Documentation, to the extent that Password Boss makes them generally available to its customers. Company may contact Password Boss in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Company shall reimburse Password Boss for any time expended for any such on-site audit at the Password Boss Group's then-current professional services rates, which shall be made available to Company upon request. Before the commencement of any such on-site audit, Company and Password Boss shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Company shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Password Boss. Company shall promptly notify Password Boss and provide information about any actual or suspected non-compliance discovered during an audit. The provision in this section shall by no means derogate from or materially alter the provisions on audits as specified in the Standard Contractual Clauses.

25. Data Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Password Boss to Company only upon Company's request.

26. Order of Precedence. This DPA is incorporated into and forms part of the Agreement. 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 prevail.

Agreed by Company:

Signature: _____

By: _____

Title: _____

Date: _____

Agreed by PasswordBoss, LLC:

Signature: *Steve Wise*

By: Steve Wise

Title: CEO

Date: March 1, 2019



Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel.: ; fax: ; e-mail:

(the data **exporter**)

And

Name of the data importing organisation: PasswordBoss, LLC

Address: 2751 Hennepin Ave S #252, Minneapolis, MN 55408, USA

Tel.:1-952-657-7855; fax: 1-952-657-7855; e-mail: dpa@passwordboss.com

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) '*personal data*', '*special categories of data*', '*process/processing*', '*controller*', '*processor*', '*data subject*' and '*supervisory authority*' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) '*the data importer*' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) '*the subprocessor*' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) '*technical and organisational security measures*' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire

legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Signature.....

On behalf of the data importer:

Name (written out in full): Steve Wise

Position: CEO

Address: 2751 Hennepin Ave S #252, Minneapolis, MN 55408, USA

Signature...*Steve Wise*

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data exporter is the legal entity that has executed the Data Processing Addendum based on the Standard Contractual Clauses as a Data Exporter established within the European Economic area and Switzerland that have purchased the Service on the basis of one or more Order(s).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Data importer, PasswordBoss, LLC, is an identity and password management cloud service provider which Processes Personal Data, where such data is Company Data, upon the instruction of the data exporter in accordance with the terms of the Agreement and the Data Processing Addendum.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

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

- Company's, business partners, and vendors of the data exporter (who are natural persons)
- Employees or contact persons of data exporter customer's, business partners, and vendors
- Employees, agents, advisors, contractors, or any user authorized by the data exporter to use the Service (who are natural persons)

Categories of data

The Personal Data transferred concern the following categories of data (please specify):

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

- First and last name
- Business contact information (company, email, phone, physical business address)
- Personal contact information (email, cell phone)
- Title
- Position Employer ID data
- Professional life data

- Personal life data (in the form of security questions and answers)
- Connection data
- Localization data

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify):

Data exporter may submit special categories of data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include Personal Data concerning health information.

Processing operations

The Personal Data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by the data importer is the performance of the Service pursuant to the Agreement.

DATA EXPORTER:

Name: _____

Authorised Signature: _____

DATA IMPORTER:

Name: Steve Wise, CEO

Authorised Signature: Steve Wise

[Remainder of this page intentionally left blank]

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

1. Technical and Organizational Security Measures

Password Boss shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Company Data, including Personal Data, as set forth in the Trust & Compliance Documentation. Password Boss regularly monitors compliance with these safeguards. Password Boss will not materially decrease the overall security of the Service during a subscription term.

DATA EXPORTER:

Name: _____

Authorised Signature: _____

DATA IMPORTER:

Name: Steve Wise, CEO

Authorised Signature: Steve Wise

Remainder of this page intentionally left blank

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

1. Sub-processors. Password Boss Use of Sub-Processors. Customer consents to Password Boss’s appointment of Subcontractors, including Sub-processors, to perform the Services. Where a Sub-processor will process Personal Data which is subject to EU Data Protection Laws, Password Boss will ensure that the Sub-processor is subject to contractual obligations regarding Personal Data which satisfy the requirements of EU Data Protection Laws. Password Boss will list its current Sub-processors at: <https://www.passwordboss.com/legal/vendors> or another link provided by Password Boss from time to time. Password Boss will remain liable for all acts or omissions of its Subcontractors or Sub-processors, and for any subcontracted obligations.

2. Security Incidents. Password Boss will promptly, and without undue delay, notify Customer if a Security Incident occurs, so long as applicable law allows this notice. Password Boss may limit the scope of, or refrain from delivering, any disclosures to the extent reasonably necessary to avoid compromising the integrity of Password Boss's security, an ongoing investigation, or any customer’s or end user's data. “Security Incident” means any actual unauthorized disclosure of or access to Customer Data, or compromise of Password Boss’s systems that Password Boss determines is reasonably likely to result in such disclosure or access, caused by failure of Password Boss's Security Measures and excluding any unauthorized disclosure or access that is caused by Customer or its End Users, including Customer or its End Users' failure to adequately secure equipment or accounts.

DATA EXPORTER:

Name: _____

Authorised Signature: _____

DATA IMPORTER:

Name: Steve Wise, CEO

Authorised Signature: *Steve Wise*