GDPR Data Processing Agreement

Last Updated: January 14, 2020

This GDPR Data Processing Addendum ("DPA") forms part of the Terms of Service or other written or electronic agreement(s) between KnowBe4, Inc. and/or its Affiliates ("KnowBe4") and Customer for the provision of products and/or services by KnowBe4 to Customer (the "Agreement"). This DPA shall reflect the parties' agreement with regard to the processing of Personal Data (as defined below) in the performance of the Agreement. By executing this DPA, Customer enters into this DPA on behalf of itself and in the name and on behalf of its Affiliates, if and to the extent KnowBe4 processes Personal Data for which such Affiliates qualify as the Controller. For the purposes of this DPA, and except where indicated otherwise, the term "Customer" shall mean the organization entering into this DPA and shall include its Affiliates, as applicable. Customer and KnowBe4 may be referred to in this DPA individually as a "party" or jointly as the "parties."

HOW TO EXECUTE THIS DPA:

To execute this DPA, Customer must:

1. Download the PDF version of the DPA for completion;
2. Fill in the information requested in the signature block and any areas requesting Customer's information; and
3. Send the signed DPA to KnowBe4 by email to privacymanager@knowbe4.com indicating Customer's full legal name and whether Customer is a current customer or prospective customer of KnowBe4.

If accepted, KnowBe4 will return the fully executed DPA to Customer. This DPA will not become effective until: (i) the DPA is fully executed and returned to Customer; and 2) the parties have entered into an Agreement for KnowBe4's products and services.

HOW THIS DPA APPLIES:

This DPA shall only apply to Customer's Personal Data that is subject to the General Data Protection Regulation (the "GDPR"), in addition to any supplemental data protection laws enacted by EEA States.

TERMS

1. <u>Definitions</u>. Capitalized terms used and not defined in this DPA have the respective meanings assigned to them in the Agreement.

"**Affiliate**" shall mean any entity that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party. For purposes of this definition, the term "control" means the power (or, as applicable, the possession or exercise of the power) to direct, or cause the direction of, the management, governance, or policies of a given entity, directly or indirectly, through any applicable means (whether through the legal, beneficial, or equitable ownership, of more than fifty percent (50%) of the aggregate of all voting or equity interests or securities of such entity, through partnership, or through some other form of ownership interest, by contract, or other applicable legal document, or otherwise).

"**Applicable Law**" shall mean all regional, national, and international laws, rules, regulations, and standards including those imposed by any governmental or regulatory authority which apply from time to time to the person or activity in the circumstances in question.

"**Auditor**" has the meaning set forth in Section 13.2.

"**Controller**" has the meaning set forth in the applicable Data Privacy Law.

"**Customer Data**" shall mean any Personal Data that KnowBe4 processes as a Processor in providing the Services to the Customer pursuant to this Agreement.

"**Data Privacy Law**" means, as the case may be, when applicable, EU General Data Protection Regulation 2016/679 ("**GDPR**"), the implementing acts of the foregoing by the Member States of the European Union and/or any other Applicable Law or regulation relating to the protection of Personal Data, personally identifiable information or protected health information.

"**Data Processing Agreement**" has the meaning set forth in the Preamble.

"**Data Subject**" has the meaning set forth in the applicable Data Privacy Law.

"**Effective Date**" shall mean the date of execution of this DPA in accordance with the above (the "Effective Date").

"**European Commission**" means an institution in the context of European Union Law.

"**Member State**" means a member state of the European Union and/or the European Economic Area, as may be amended from time to time.

"**Personal Data**" has the meaning set forth in the applicable Data Privacy Law.

"**Privacy Shield Framework**" means the EU-US and/or Swiss-US Privacy Shield self-certification program operated by the US Department of Commerce.

"**Privacy Shield Principles**" shall mean the Privacy Shield Framework Principles (as supplemented by supplemental principles).

"**Process**" has the meaning set forth in the applicable Data Privacy Law.

"**Processing**" has the correlative meaning to Process as set forth in the applicable Data Privacy Law.

"**Processor**" has the meaning set forth in the applicable Data Privacy Law.

"**Security Incident**" has the meaning set forth in Section 7.1.

"**Services**" means the provision of products, services or other work products by KnowBe4 as described and set out in the Agreement, and such other services as the parties may agree upon in writing from time to time.

"**Subprocessor**" means a third party, other than an Affiliate, engaged by KnowBe4 to assist with the provision of the Services which involves the processing of Customer Data.

"**Term**" is the term of the Agreement.

2. **Relationship with Agreement.** In the event of a conflict or inconsistency between the provisions in the Agreement and this DPA, the provisions of this DPA shall take precedence solely to the extent this DPA requires additional, more stringent, or more protective obligations, otherwise all provisions of the Agreement shall apply.

3. **Status of Parties.** KnowBe4 is the Processor of Customer Data and Customer is the Controller of Customer Data under this DPA. KnowBe4 shall not assume any responsibility for determining the purposes for which Customer Data shall be processed.

4. **Scope of Data Processing.**

4.1. All parties shall comply with their applicable obligations under Data Privacy Laws.

4.2. The subject-matter of the data processing to be carried out by KnowBe4 is: *Current employees and contractors of the Customer.*

4.3. The duration of the data processing to be carried out by KnowBe4 shall be for the Term stated in the Agreement.

4.4. The nature of the data processing to be carried out by KnowBe4 is: *For the delivery and use of the Services provided by KnowBe4. KnowBe4 is in the field of providing web-based services for simulated security testing (such as simulated phishing), security awareness training, compliance training, governance, risk and compliance management, and other tools and features related to the aforementioned fields.*

4.5. The purpose of the data processing is: *The purpose of Processing Customer Data by KnowBe4 is for the performance of the Services pursuant to the Agreement including: storage; access for customer service and support; providing Customer access and use of the Services; abuse detection, prevention, and remediation; and maintaining, improving, and providing the Services.*

4.6. The type of personal data involved in the data processing is: The personal data transferred concern the following categories of data (please specify): *name, email address, telephone number, title, training and testing results/metrics, IP addresses, and web browser information.*

4.7. The categories of Data Subjects involved in data processing are: *Current employees and contractors of the Customer.*

5. <u>Processor Obligations</u>.

5.1. KnowBe4 shall process Customer Data on behalf of Customer exclusively and only in accordance with the documented instructions received from Customer, including in accordance with the Agreement. Customer may provide KnowBe4 with general or specific instructions regarding the data processing provided as part of the Services. Instructions shall be issued in writing or via email.

5.2. Customer shall only provide instructions to KnowBe4 that comply with Applicable Law and Customer represents and warrants that KnowBe4's Processing in accordance with Customer's instructions shall not cause KnowBe4 to be in breach of any Applicable Laws.

5.3. KnowBe4 shall promptly notify Customer if KnowBe4 reasonably believes that an instruction issued Customer would violate any Data Protection Laws.

5.4. If KnowBe4 cannot provide compliance with this DPA for whatever reason, then it shall promptly inform Customer of its inability to comply, in which case the parties shall negotiate in good faith alternative Processing and, if no other alternative processing is commercially reasonable to the Provider, the Provider may immediately suspend any processing and/or terminate, in whole or in part, the Agreement and this DPA pursuant to the Agreement.

5.5. Upon Customer's request, KnowBe4 will cooperate with Customer to enable Customer to: (a) comply with reasonable requests of access, rectification, and/or deletion of Customer Data arising from a Data Subject; (b) enforce rights of Data Subjects under the Data Privacy Law; and/or (c) comply with all requests from a supervisory authority, including but not limited to in the event of an investigation. All costs of such cooperation shall be borne by the Customer.

5.6. KnowBe4 shall provide commercially reasonable assistance to Customer where Customer carries out a data privacy impact assessment relating to Customer Data.

5.7. KnowBe4 shall notify Customer in the event it receives any request, complaint, or communication relating to Customer's obligations under Data Privacy Laws (including from data protection authorities and/or supervisory authorities). To the extent permitted by Applicable Law, KnowBe4 shall obtain specific written consent and instructions from Customer prior to responding to such request, complaint, or communication.

5.8. Any data collected pursuant to data analytics or monitoring carried out by KnowBe4 in connection with the provision of the Services or otherwise connected with Customer's use of the Services may include Personal Data, which Customer hereby authorizes KnowBe4 to use solely in accordance with carrying out its obligations under the Agreement or this DPA.

6. Scope Modifications.

6.1. In the event that changes in Data Privacy Laws require modifications to the Services, the parties shall use commercially reasonable efforts to comply with such requirements. If such changes in Data Privacy Laws require structural changes to the Services such that the provision of the Services would otherwise be in breach of such Data Privacy Laws unless such changes are performed, the parties will discuss in good faith KnowBe4's ability to comply and will negotiate and revise the Agreement, DPA or otherwise modify the provision of Services accordingly. In the event that KnowBe4 considers in good faith that it is unable to comply with the required changes, KnowBe4 shall notify Customer without undue delay and KnowBe4 may terminate the Agreement and/or this DPA on no less than thirty (30) days' prior written notice.

6.2. In the event that a party's compliance with Data Privacy Laws requires the imposition of certain additional contractual obligations under this DPA, such party shall notify the other party and both parties shall in good faith seek to amend this DPA in order to address the requirements under Data Privacy Laws. In the event the affected parties fail to reach agreement on an amendment to this DPA, then the parties may, on no less than two (2) months' prior written notice, terminate the Agreement and this DPA.

6.3. Customer shall notify KnowBe4 of any faults or irregularities in relation to this DPA that it detects in the provision of the Services.

7. Security Measures.

7.1. KnowBe4 shall take and implement appropriate technical and organizational security and confidentiality measures designed to provide a level of security appropriate to the risk to Customer Data against unauthorized use, modification, loss, compromise, destruction, or disclosure of, or access to, Customer Data (a "**Security Incident**").

7.2. Such measures implemented in Section 7.1 shall require KnowBe4 to have regard to industry standards and costs of implementation as well as taking into account the nature, scope, context, and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals.

7.3. KnowBe4 shall undertake regular reviews of the technical and organizational measures and the data processing operations connected with the Services to ensure compliance with the DPA and to consider improving the technical and organizational measures such that they meet or exceed the requirements of the Agreement.

7.4. KnowBe4 shall adopt and maintain a comprehensive written information security policy that describes its policies and procedures to comply with this Section 7 and shall provide a summary of such policy to Customer upon request. Information about KnowBe4's information security practices can be found at at https://www.knowbe4.com/security, or such other URL locations on KnowBe4's website as KnowBe4 may provide from time to time.

7.5. KnowBe4 shall implement and maintain policies and procedures to detect and respond to Security Incidents.

7.6. For the Term of the Agreement, KnowBe4 will ensure that all persons authorized to process Customer Data only processes Customer Data in accordance with instructions from Customer (unless required to do otherwise under Applicable Law).

8. Confidentiality.

8.1 "**Confidential Information**" means all information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information of Customer includes Customer Data. Confidential Information of KnowBe4 includes, without limitation, the Services, information about KnowBe4's infrastructure or network, KnowBe4's list of Subprocessors, information about KnowBe4's internal security or privacy controls or policies, KnowBe4's technical and organizational measures, the results or findings of any audit or investigation, KnowBe4's SOC report(s), and other information or documentation received by Customer in the evaluation of KnowBe4's Services. Confidential Information of each party includes business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such party. However, Confidential Information does not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party. For the avoidance of doubt, the non-disclosure obligations set forth in this "Confidentiality" section apply to Confidential Information exchanged between the parties in connection with the evaluation of additional KnowBe4 services.

8.2 As between the parties, each party retains all ownership rights in and to its Confidential Information. The Receiving Party will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but not less than reasonable care) to (i) not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this DPA and (ii) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and contractors who need that access for purposes consistent with this Agreement and who are bound by obligations of confidentiality or have signed confidentiality agreements with the Receiving Party containing protections not materially less protective of the Confidential Information than those herein. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of the compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to that Confidential Information.

9. <u>Security Incident Notification Obligations</u>.

9.1. In the event of a Security Incident arising during the performance of the Services by KnowBe4, KnowBe4 shall:

(a) notify Customer about the Security Incident without undue delay after becoming aware of the Security Incident;

(b) as part of the notification under Section 9.1(a), to the extent reasonably available at the time of notice, provide a description of the Security Incident including the nature of the Security Incident, the categories and approximate number of Data Subjects affected, the categories and approximate number of data records affected, the likely consequences of the Security Incident and the risks to affected Data Subjects;

(c) promptly update Customer as additional relevant information set forth in 9.1(b) above become available;

(d) take all actions as may be required by Data Privacy Laws;

(e) maintain records of all information relating to the Security Incident, including the results of its own investigations and authorities' investigations as well as remedial actions taken; and

(f) reasonably cooperate with Customer to prevent future Security Incidents.

9.2. KnowBe4 shall make any information referred to under Section 9.1 available to Customer upon request. All such information shall be considered Confidential Information of KnowBe4.

10. Subprocessors.

10.1. Controller authorizes KnowBe4 to appoint (and permit each Subprocessor appointed in accordance with this Section 10 to appoint) Subprocessors in accordance with this Section 10 and any restrictions in the Agreement.

10.2. Notwithstanding anything to the contrary in this DPA or the Agreement, KnowBe4 may continue to use all Subprocessors (including Affiliates) already engaged by KnowBe4 as of the Effective Date, subject to KnowBe4 promptly meeting the obligations set forth in Section 10.4. Customer may request a list of KnowBe4's current Subprocessors by emailing privacymanager@knowbe4.com, provided Customer has executed this DPA or upon the execution of an agreement with KnowBe4 containing obligations of confidentiality.

10.3. KnowBe4 shall provide reasonable advanced notification to Customer where KnowBe4 wishes to engage a Subprocessor to process Customer Data and shall provide, upon Customer's request, the identity and location of the Subprocessor and a description of the processing to be subcontracted or outsourced to such Subprocessor. Where KnowBe4 wishes to appoint a Subprocessor under this DPA, KnowBe4 will select the Subprocessor with due diligence and will verify prior to engaging the Subprocessor that such Subprocessor is capable of complying with the obligations of KnowBe4 towards Customer, to the extent applicable to the Services assigned to that Subprocessor. If, within five (5) days of receipt of such notice, Customer notifies KnowBe4 in writing of any objections (on reasonable grounds) to the proposed appointment, then KnowBe4 shall not appoint (or disclose any Customer Data to) the proposed Subprocessor until reasonable steps have been taken to address the reasonable objections raised by Customer, and KnowBe4 has been provided a reasonable written explanation of the steps taken.

10.4. KnowBe4 shall enter into a contract with each Subprocessor whereby KnowBe4 shall require the Subprocessor to comply with obligations no less onerous than KnowBe4's obligations under this DPA. KnowBe4 shall ensure the subcontracting agreement with such Subprocessor includes appropriate contractual provisions in accordance with Data Privacy Laws.

10.5. Such subcontracting under this Section 10 shall not release KnowBe4 from its responsibility under the Agreement. KnowBe4 shall be responsible for the work and activities of all Subprocessors.

11. International Data Transfers. Customer acknowledges that in the event that KnowBe4's Services are covered by more than one transfer mechanism, the transfer of Customer Data will be subject to a single transfer mechanism in the following order of precedence: (i) KnowBe4's EU-US and Swiss-EU Privacy Shield Framework self-certifications; (ii) the Standard Contractual Clauses or such other adequate data transfer mechanism(s) as entered into by the parties.

11.1 The parties further agree that the Privacy Shield Framework will be the lawful transfer mechanism Customer Data from the EEA or Switzerland to KnowBe4 in the United States. KnowBe4 represents that it is self-certified to the Privacy Shield Framework and agrees, with respect Customer Data, that it shall comply with the Privacy Shield Principles when handling any such data.

11.3 If for any reason the aforementioned data transfer mechanisms are deemed inadequate by the appropriate regulatory body such as the European Commission, the parties will show good faith to enter into the appropriate data transfer mechanism(s) pursuant to Article 46 of the GDPR. This may include, but is not limited to, data protection certification and seals and marks.

12. Return and Destruction.

12.1. Without prejudice to any obligations under this Section 12, following termination or expiration of the Agreement for whatever reason, KnowBe4 shall cease processing Customer Data and shall require that all Subprocessors cease processing Customer Data.

12.2. Following termination or expiration of the Agreement for whatever reason and having received written confirmation from Customer, KnowBe4 shall destroy all copies of Customer Data, unless and for the duration KnowBe4 is permitted to retain such Customer Data in accordance with Applicable Laws. Notwithstanding the foregoing, to the extent it is not commercially reasonable for KnowBe4 to remove Customer Data from archive or other backup media, KnowBe4 may retain Customer Data on such media in accordance with its backup or other disaster recovery procedures. In the event KnowBe4 retains Customer Data after the Term, KnowBe4 shall continue to comply with the confidentiality and privacy obligations hereunder until it is no longer in possession of Customer Data.

12.3. To the extent feasible, KnowBe4 shall archive documentation that is evidence of proper Customer Data processing beyond termination or expiration of the Agreement and continuing for any period of time in which KnowBe4 retains Customer Data.

12.4. KnowBe4 may retain Customer Data where strictly required to store such data under Applicable Law and for legitimate business purposes.

13. Audits.

13.1. KnowBe4 shall, upon receiving at least thirty (30) days prior written notice from Customer, submit its data processing facilities for a reasonable audit of Processing activities carried out under this DPA, where such audit shall be carried out by an independent third-party auditor mutually agreed upon by the parties and bound by a duty of confidentiality ("**Auditor**") and, where applicable, approved by the relevant supervisory authority. Any effort as well as internal and external costs of audits requested by Customer pursuant to this Section shall be borne by the Customer.

13.2. KnowBe4 shall provide Customer or Auditor with the necessary information and shall keep the necessary records required for an audit of the processing of Customer Data and will, subject to Applicable Law, provide said documents and/or data media to Customer upon written request.

13.3. KnowBe4 shall provide reasonable support for any and all audits of Customer or Auditor under this Section and shall contribute to the complete and efficient completion of the audit.

13.4 Such audit is subject to the following conditions: (i) audits are limited to KnowBe4's facilities and personnel of the KnowBe4 in scope of this DPA; (ii) audits occur no more than once annually; and (iii) may be performed during regular business hours, without substantially disrupting the KnowBe4's business operations in accordance with the KnowBe4's security policies. Customer may create an audit report summarizing the findings and observations of the audit ("**Audit Report**"). Audit Reports are confidential information of the KnowBe4 and the Customer will not disclose them to third parties except for the Customer's legal counsel and consultants bound by obligations of confidentiality.

14. Termination. The rights of termination for cause as set out in the Agreement remain unaffected. The termination or expiration of the Agreement for any reason shall cause termination of this DPA.

15. Liability. The liability of each party under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement. Any reference to any "limitation of liability" of a party in the Agreement shall be interpreted to mean the aggregate liability of a party and all of its Affiliates under the Agreement and this DPA.

16. Miscellaneous.

16.1. **Amendment.** This DPA may not be amended or modified except in writing signed by authorized representatives of both parties.

16.2. **Severability.** If any provision in this DPA is determined to be ineffective or void by any court or body of competent jurisdiction or by virtue of any legislation to which it is subject, it shall be ineffective or void to that extent only and the validity and enforceability of the remaining provisions of the DPA and the Agreement shall not be affected. The parties shall promptly and in good faith work to replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. The parties shall similarly promptly and in good faith add any necessary appropriate provision where such a provision is found to be missing by any court or body of competent jurisdiction or by virtue of any legislation to which this DPA is subject.

16.3. **Governing Law.** Notwithstanding anything to the contrary in the Agreement, this DPA shall be governed by and construed in accordance with the national law that applies to the Controller.

16.4. **Headings.** The headings in this DPA are for reference only and shall not affect the interpretation of this DPA.

16.5 **Notices**. For notices related to this DPA, Customer may send an email to privacymanager@knowbe4.com. Alternatively, Customer may send notice by way of mail at the address listed below. All notices to Customer will be addressed to the relevant account administrator designated by Customer.

Notice address for KnowBe4:
KnowBe4, Inc.
Attn: Legal Department
33 N. Garden Ave., Suite 1200
Clearwater, Florida, U.S.A. 33755
privacymanager@knowbe4.com

CUSTOMER

Signature: _____

Customer Legal Name: _____

Print Name: _____

Email: _____

Title: _____

Date: _____

KNOWBE4, INC.

Signature: _____

Print Name: _____

Title: _____

Date: _____