GDPR Data Processing Addendum

Last Updated: July 17, 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 this 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 privacy@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 (including any attachments) 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. Definitions. 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 Protection 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 Protection 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 Protection 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 Protection Law.

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

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

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

"**Standard Contractual Clauses**" has the meaning set forth in Section 11.

"**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 Protection 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. Processor Obligations.

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 Protection 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 Protection 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 Protection Laws require modifications to the Services, the parties shall use commercially reasonable efforts to comply with such requirements. If such changes in Data Protection Laws require structural changes to the Services such that the provision of the Services would otherwise be in breach of such Data Protection 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 Protection 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 Protection 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. Security Incident Notification Obligations.

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 Protection 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 privacy@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 Protection 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.

11.1 **Standard Contractual Clauses**. This DPA hereby incorporates by reference the Standard Contractual clauses for data controller to data processor transfers approved by the European Commission in decision 2010/593/EU, provided that Appendices 1 and 2 of the Standard Contractual Clauses are set forth in Attachment 1 to this DPA. The parties further agree that the Standard Contractual Clauses will apply to personal data that is transferred via the Services from the European Economic Area, the United Kingdom, and/or Switzerland to outside the European Economic Area, the United Kingdom, and Switzerland, either directly or via onward transfer, to any country or recipient not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive).

11.2 If for any reason the aforementioned data transfer mechanism is 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 privacy@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
privacy@knowbe4.com

KNOWBE4

By: _____
Name: _____
Title: _____
Date: _____

Address for notices:
33 N. Garden Ave Suite 1200
Clearwater, Florida, USA 33755
E-mail: privacy@knowbe4.com
Phone: (855) 566-9234
Attention: Legal Department

CUSTOMER *(Full Legal Name)*: _____

By: _____
Name: _____
Title: _____
Date: _____

Address for notices:

_____

_____

E-mail: _____
Phone: _____
Attention: _____

Attachment 1

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
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

The Customer, as defined in GDPR Data Processing Addendum (the "data exporter")

And

Name of the data importing organisation: KnowBe4, Inc. and/or its affiliates

Address: 33 North Garden Ave., Suite 1200, Clearwater, FL 33755, U.S.A.

Tel.: 855-566-9234; e-mail: privacy@knowbe4.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 of 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 establishe.

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.

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):
An individual or entity that has contracted with KnowBe4 for security awareness training and/or simulated phishing services.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):
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 that allow users to store, create, send, and track results of training campaigns and/or simulated phishing campaigns and allow users to store, create, send, and track results and other metrics related to governance, risk and compliance management.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):
Current employees and contractors of the Customer.

Categories of data

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

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):
None.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):
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.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Information Security Requirements

1. Security Mission Statement

KnowBe4 represents and warrants that it has developed, implemented and will maintain a comprehensive, written information security program that requires the implementation of administrative, physical and technical safeguards to protect Personal Data against unauthorized or inappropriate use, access or transmission, regardless of whether such Personal Data is received by KnowBe4 from Customer, is collected by KnowBe4 on behalf of Customer, is generated by KnowBe4 on behalf of Customer, or where access has been granted to KnowBe4 by or at the direction of Customer. KnowBe4 shall ensure that all such safeguards, including the manner in which Personal Data is collected, accessed, used, stored, processed, disposed of and disclosed, are no less rigorous than industry standards that comply with Applicable Data Protection Law, as well as the terms and conditions of this Agreement.

2. Organizational Security: KnowBe4 represents and warrants that it has in place an organizational security policy to ensure the confidentiality, integrity, and availability of Personal Data.

i. **Information Security Program:** KnowBe4's written information security program will require that KnowBe4 apply the same level of security to Personal Data as KnowBe4 would provide for its own proprietary, sensitive and confidential information.

ii. **Access Controls:** KnowBe4 implements access controls, including appropriate authentication and credential protocols, and limits access to only authorized representatives who need to access the Personal Data in order to: (i) carry out their obligations under the Agreement; (ii) safeguard the physical location and infrastructure of any database or record storage area; and (iii) safeguard the transmission or transport of any records, including appropriate encryption standards for electronic transmission.

iii. **Cyber Incident Strategy:** KnowBe4 maintains a cyber-incident mitigation strategy, including identifying root cause analysis, internal escalations and risk assessment and the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and maintain a cyber-incident response plan.

iv. **Data Restriction:** the duration of access shall be restricted to the minimum time for which access is required. KnowBe4 shall use safeguards to protect against any compromise, unauthorized access or other damage to Customer's network and to secure its networks and IT environments associated with the services being provided to Customer.

3. Oversight of Compliance. KnowBe4 shall regularly, but not less than annually, evaluate, test and monitor the effectiveness of its written information security program and shall promptly adjust and/or update as reasonably warranted by the results of such evaluation, testing, and monitoring.

i. **Compliance Requirements:** KnowBe4 shall provide, upon request, a controls audit report and remediation effort, such as a SOC 2 Type 2 reports or information security audit as applicable to the services being provided, which has been performed within the past year by an independent third-party. The audit shall include an assessment of KnowBe4's applicable general controls and security processes and procedures to ensure compliance with Applicable Laws, regulations and industry standards.

ii. **Information Security Audit Requirements:** The audit shall specifically address at a minimum the security of the system to ensure it is protected against unauthorized access (both physical and logical).

iii. **Optional Requirements:** At KnowBe4's discretion the information security audit shall optionally address: (i) the availability of the system; (ii) the processing integrity of the system; (iii) the confidentiality of the system; and (iv) the privacy of the system.

iv. **Record Retention and Data de-identification:** KnowBe4 shall maintain a records retention policy, which ensures secure storage and destruction, in accordance with the requirements of the Agreement or instructions from Customer. Ensure the pseudonymization or encryption of Personal Data where appropriate. KnowBe4 shall de-identify all Personal Data prior to storing, accessing, or processing Personal Data in environments other than production environments.

v. **Application Architecture Diagram with Data Flows.** Customer may request a copy of KnowBe4's current application architecture diagram with data flows by emailing privacy@knowbe4.com, provided Customer has executed this DPA or upon the execution of an agreement with KnowBe4 containing obligations of confidentiality. In order to request KnowBe4's current application architecture diagram in advance to signing this DPA, you may submit your request along with a signed copy of KnowBe4's non-disclosure agreement to privacy@knowbe4.com.

4. Security Incident. KnowBe4 shall promptly notify Customer (and in any event, no later than 72 hours) of any Security Incident. KnowBe4 shall not inform any third party of any Security Incident except as may be strictly required by Applicable Law, without first obtaining Customer's prior written consent.

i. **General Requirements:** KnowBe4 shall promptly remedy any Security Incident and prevent any further Security Incident at KnowBe4's expense in accordance with applicable privacy rights, laws, regulations and standards.

ii. **Obligations to Customer:** KnowBe4 shall cooperate fully with Customer in the investigation and response to any Security Incident, including the name and contact information for KnowBe4's primary security contact who shall be available to assist

Customer during reasonable days and times as a contact in resolving obligations associated with a Security Incident. In addition, KnowBe4 agrees to: (i) assist with any investigation; (ii) facilitate interviews with KnowBe4's employees and others involved in the matter; and (iii) make available all relevant records, logs, files, data reporting and other materials required to comply with Applicable Law, regulation, industry standards or as otherwise required by Customer.

5. Handling of Personal Data. Unless otherwise agreed in advance by the Customer in writing, all Personal Data shall be encrypted during storage, transmission, and processing, using standards consistent with industry standards and all Applicable Laws, including but not limited to the Applicable Data Protection Laws.

i. **Information Security Monitoring.** KnowBe4 shall maintain, regularly monitor (but in no event less than once per year) and enforce policies that:

a. require its personnel, and those of KnowBe4's subcontractors, that have access and are able to copy or download any Personal Data to encrypt all Personal Data stored on all digital or electronic portable storage devices (including computer laptops, iPads or other tablets, PDAs, CDs, diskettes, portable drives, magnetic tapes and other similar devices) where such devices are capable of such encryption; and

b. prohibit such personnel from storing any Personal Data on any such devices that are not capable of encryption.

ii. **Deletion of Data**. At any time during the term of this Agreement, at Customer's request, or immediately upon the termination or expiration of this Agreement, upon Customer's request, KnowBe4 shall promptly destroy all records and data not contained within audit trails or backups containing Personal Data. Customer may request a certificate of secure destruction evidencing such actions taken by KnowBe4. Customer acknowledges some Personal Data may be required in order for KnowBe4 to fully perform its Services under the Services Agreement. Personal Data contained within audit trail logs and database backups that must be retained in accordance with KnowBe4 data retention policies shall continue to be protected under the full terms and conditions of this DPA.