Global Data Processing Addendum

Last Updated: February 7, 2023

This Global Data Processing Addendum ("DPA") forms part of the Terms of Service or other written or electronic agreement(s) between KnowBe4, Inc. and/or its subsidiaries ("KnowBe4" or "Service Provider") 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 dpa@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 to the extent that it is subject to applicable Data Protection Law as defined in the DPA.

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 Singapore's Personal Data Protection Act of 2012, Act on Protection of Personal Information ("APPI") of Japan, Lei Geral De Proteção De Dados ("LGPD") of Brazil, Protection of Personal Information Act (POPIA) of South Africa, 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.

"International Data Transfer Addendum ("IDTA")" means the international data transfer addendum approved by the United Kingdom's parliament currently located here where Service Provider is Processor and Customer is Controller.

"**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, third party integration data; and coaching and training 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 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, but not later than twenty-four (24) hours, 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 dpa@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 a list of KnowBe4's current Subprocessors before execution of this DPA, you may submit your request along with a signed copy of

KnowBe4's non-disclosure agreement to dpa@knowbe4.com. A copy of KnowBe4's non-disclosure agreement may be downloaded here.

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 fifteen (15) 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 **European Economic Area ("EEA")**. This DPA hereby incorporates by reference the Standard Contractual clauses for data controller to data processor transfers approved by the European Commission in decision 2021/914 of June 4 2021 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 and/or Switzerland to outside the European Economic Area 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 **United Kingdom**. The IDTA will apply to Customer Data that is transferred via the Services from the United Kingdom to outside the United Kingdom, either directly or via onward transfer, to any country or recipient not recognized by United Kingdom regulatory authorities as providing an adequate level of protection for personal data (as described in Data Protection Law).

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.

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, unless there is a material breach of this Agreement or a Security Incident; 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 dpa@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.

KNOWBE4		**CUSTOMER:** _____ *(full legal entity name)*	
Signature:		**Signature:**	
Name:		**Name:**	
Title:		**Title:**	
Date:		**Date:**	
Address for Notices:		**Address for Notices:**	
	33 N. Garden Ave., Suite 1200		
	Clearwater, Florida 33755 USA		
E-mail:	legal@knowbe4.com	**E-mail:**	
Phone:	(855) 566-9234 ext. 102	**Phone:**	
Attention:	Legal Department	**Attention:**	

STANDARD CONTRACTUAL CLAUSES

(C2P)

SECTION I

Clause 1.

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) [(1)] for the transfer of personal data to a third country.

(b) The Parties.

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2.

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided, however, that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3.

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4.

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5.

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6.

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7.

[INTENTIONALLY BLANK]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8.

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1. Instructions.

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2. Purpose limitation. The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3. **Transparency.** On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4. **Accuracy.** If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5. **Duration of processing and erasure or return of data.**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6. **Security of processing.**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7. **Sensitive data.**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8. **Onward transfers.**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. Documentation and compliance.

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9.

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fifteen (15) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects[3]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

---

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10.

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraph (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11.

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[4] at no cost to the data subject. It shall inform the data subjects, in the manner set out in this paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12.

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

---

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13.

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14.

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination including those requiring the disclosure of data to public authorities or authorising access by such authorities relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[5];

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (c), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15.

Obligations of the data importer in case of access by public authorities

15.1. Notification.

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraph (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) paragraph (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

---

conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

15.2. Review of legality and data minimisation.

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16.

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (a) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17.

Governing law

(a) These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of another EU Member State mutually agreed upon by both parties.

Clause 18.

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the EU Member State of which the data exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex 1

Data exporter(s):

1. Name: As specified in the recital of the DPA.

   Address: As specified in the recital of the DPA.

   Contact person's name, position and contact details: This shall be the main point of contact for the Customer.

   Activities relevant to the data transferred under these Clauses: Simulated Phishing and Security Awareness Training and/or governance risk and compliance services.

   Role (controller/processor): *Controller*

Data importer(s):

1. Name: *KnowBe4, Inc.*

   Address: *33 N Garden Ave, Suite 1200, Clearwater, FL, 33755*

   Contact person's name, position and contact details: *privacy@knowbe4.com*

   Activities relevant to the data transferred under these Clauses: *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.*

   Role (controller/processor): *Processor*

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Current employees and contractors of the customer

Categories of personal data transferred

Data Collected Directly from Customer:

First Name, Last Name, Manager First Name, Manager Last Name, Business Phone Number, Mobile Phone Number, Employee Title, Employee Department, IP address, browser information; Third Party Integration Data

Generated Information:

Phishing Campaign Results and Metrics; Security Awareness Training Results; Risk Score; Training and Coaching Information

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Frequency of data transfer will be on a continuous basis throughout the duration of the Services.

Nature of the processing

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.

Purpose(s) of the data transfer and further processing

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.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

KMSAT Console (including its components such as PhishRIP, PhishER, PhishML etc.): Account and associated data permanently deleted after termination and 18 months of account inactivity. Backups are stored for (1) one year and audit trails for (3) three years

KCM GRC: KCM GRC accounts can only be deleted upon request. If you wish to have your KCM GRC account deleted, please submit a request to your CSM. Database Backups are stored for (1) one year and audit trails for (3) three years

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

To provide infrastructure for the Services, product functionality, including application and system logging, and analytics, and support services, including tracking of support requests, and analyzing, measuring and improvement of customer experience. Duration of this processing will be for the duration of the Services as described in the Agreement.

COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The data protection authorities of the locations of which the data exporter is established.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Applicable Products:

1. **Access control to premises and facilities**

Unauthorized access (in the physical sense) must be prevented.

Physical security controls where data is stored are implemented by the data center provider, Amazon. KnowBe4 operates Amazon Web Services (AWS) servers at various global locations.. The data storage locations for KnowBe4 can be found here: https://support.knowbe4.com/hc/en-us/articles/1500007523981-KnowBe4-Sub-Processors. KnowBe4 has reviewed the security due diligence information including the SOC 2 Type 2 assessment of Amazon Web Services Data Center physical security controls and found them to be more than adequate.

The KnowBe4 HQ has access controls such as fingerprint readers, motion detectors, video monitoring and additional physical security controls implemented. No customer data is stored within the KnowBe4 office. Entrances to the KnowBe4 suites are controlled by a biometric access system. Employees and contractors who need access to the offices are registered in the system and their fingerprints are recorded.

After hours access to the KnowBe4 suits requires a key fob for access to the building or use of a PIN for the elevator access to the suites.

Visitors are required to sign-in at the reception desk and wear a visitor badge while on-site all the time.

A security camera system is in place that records all access to and stay in the KnowBe4 suites. Security guards employed by KnowBe4 are on-site during business hours. Third party security personnel are contracted to patrol the suites after hours. A third-party alarm system is in place and continuously monitors for physical security breaches. Triggered alarms or other identified security incidents are immediately reported to on-duty security personnel and the Director of Physical Security using a dedicated phone line.

2. **Access control to systems**

Unauthorized access to IT systems must be prevented.

The KnowBe4 Training Console currently enforces a eight-character password minimum with no complexity, history, or reuse requirements. Customers who wish to control access with a stricter password complexity have the option to implement Single

Sign-On with SAML integration. SAML will allow the Customer to control the password complexity requirements within their own authentication system. KnowBe4 administrators must access the administrative portion of the console using two-factor authentication.

KnowBe4 as an organization implements a sixteen (16) character minimum password length, requires multi-factor authentication for access, and has issued a corporate managed enterprise password manager to all staff. Passwords are required to be changed once per year or with reason to believe it is not following the password policy or is known to be compromised.

KnowBe4 employees use a single sign-on provider to access applications for business purposes. Access is appropriately granted upon hire and promptly revoked upon termination via the single-sign on provider administration panel.

KnowBe4 limits the number of employees who may manage servers and deploy application code. Access uses key based authentication via SSH. All activity within the Amazon Web Services console must come from a trusted IP address of the KnowBe4 VPN. Access to the Amazon Web Services administrative console is restricted to a limited number of senior employees.

KnowBe4 has implemented a formal change management process that allows staff to request, manage, approve, and control changes that modify services or systems within the KnowBe4 environments. The change control process is designed to enforce key development controls each time a change to the software is made, including development and emergency changes. The change management process begins with the identification, recording and classification of the change, and continues with its review and approval, test, and staging for implementation. Once implementation has been completed, measured, and reported, the change process is complete.

The Engineering Development Team has been structured to promote communication through each stage in the design process. This results in the Management Team ultimately being responsible for ensuring development initiatives meet client needs and strategic direction of the application including transition from concept to production functionality. A code repository (change control software) tool is utilized and combined with documentation of each release which provides for the ability to quickly revert to a previously functioning state version in the event that new code does not function as intended at any point in the development process.

3. Access control to data

Activities in IT systems not covered by the allocated access rights must be prevented.

Access to Customer Data is available to necessary sales, support, and management staff within KnowBe4. Certain KnowBe4 employees have access to support the Customer in pre- and post- sales technical support. Access to the Customer Data is granted through a single-sign-on provider. Customers can configure their console to restrict access from KnowBe4 support staff and enable access as needed.

The ability to manage application code, servers, and databases is limited to employees with a more specific need to know. These

employees include developers and senior technical support staff. Access to servers is only available from selected trusted IP addresses and uses key based SSH authentication. Management of the AWS consoles is also limited to these individuals and requires two-factor authentication.

Customer Data is stored privately within data stores that reside in the AWS Data Center specified by the Customer. Access to the Customer Data within these data stores is only available via private VPN with MFA connections and via the application itself.

There are information security policies in place to set the overall framework for managing security of the IT infrastructure and applications. These policies are approved at executive management level and they establish standards for information security throughout KnowBe4's information resources. The Information Security Team has primary responsibility for interpreting the standards, developing procedures, and processes for implementing the standards, and overseeing the logical security of KnowBe4 IT and its applications.

Employees who no longer require access to the AWS environment are deactivated upon notification and in no case longer than 24 hours after termination. Quarterly access reviews are also performed to ensure access to systems within the environment are appropriate.

4. Disclosure control

Aspects of the disclosure of personal data must be controlled: electronic transfer, data transport, transmission control, etc.

The internal network is protected from public internet traffic via stateful inspection firewalls provided by AWS. AWS security groups act as a firewalls and control the traffic allowed into compute and storage resources . For each security group, custom rules are added that govern the allowed inbound traffic to the resources. All other inbound traffic is denied.

Encrypted communication is utilized to protect remote internet sessions to the KnowBe4 applications and internal network. Encryption is used to ensure the privacy and integrity of the data being passed over the public network.

All data is transmitted over secure channels using TLS 1.2 or higher. This includes access to the KnowBe4 Training console website, information sent to third parties for processing, and logging. Data exchanged between compute resources and data stores is done within private subnets of an AWS Virtual Private Cloud (VPC) within Amazon Web Services.

Data exchanged between the Customer and the KnowBe4 platforms is encrypted using TLS that supports TLS 1.2 and higher. The database instance is encrypted with the AES256 encryption standard using AWS KMS.

5. Input control

Full documentation of data management and maintenance must be maintained.

All actions within the KnowBe4 Training Console are attributable to a user and logged. This includes creation, deletion, modification of data as well as actions users take like logging in and accessing training material. These logs are aggregated on a central logging server (datadog) and are archived to an encrypted file storage service within the applicable AWS region that was specified originally by the Customer.

6. Job control

Commissioned data processing must be carried out according to instructions.

KnowBe4 and the Customer mutually agree to abide by the terms and conditions as outlined in the contract for services to be provided.

KnowBe4 and the Customer mutually agree and acknowledge that any and all Personal Data provided by the Customer is the responsibility of the person or entity from whom such Personal Data originated. The Customer, and not KnowBe4, is entirely responsible for all Personal Data that its users upload, post, email, transmit, store or otherwise make available via the Services described within the contract.

Any users who seek to access, or who seek to correct, amend, or delete inaccurate data may do so by contacting one of the Customer's designated administrators of the service provided.

7. Availability control

The data must be protected against accidental destruction or loss.

KnowBe4's systems run in the cloud and do not run their own routers, load balancers, DNS servers, or virtual systems. Except for a few data sub-processors, services and data, data are hosted primarily in AWS data centers. A full accounting of data processing locations can be found in the KnowBe4 subprocessor listing located at the following URL https://support.knowbe4.com/hc/en-us/articles/1500007523981-KnowBe4-Subprocessors. KnowBe4's systems are built taking into consideration both business continuity and disaster recovery. The IT infrastructure, including systems and databases, is spread across multiple AWS data centers (availability zones) for all regions for redundancy and continuity purposes. Systems are within KnowBe4's own virtual private cloud (VPC) with network access control lists (ACLs) to prevent unauthorized requests gaining access to the internal network.

KnowBe4 uses the AWS Fargate platform. AWS Fargate is a serverless computer engine for Amazon Elastic Container Service (ECS) that allows KnowBe4 to run containers without having to provision, configure, and scale clusters of Virtual Machines (VMs) or manage host operating systems. Fargate manages the underlying infrastructure and clusters. It also

automatically scales the application based on demand. Fargate eliminates the need to scale, monitor, patch, and secure traditional server instances.

Data communication between Customer and KnowBe4's backend systems are encrypted – which protects data in transit. Data is held in an encrypted data stores, which provides for availability and data durability. Encryption is enabled to protect data at rest using AWS KMS.

KnowBe4's backup and recovery infrastructure is hosted and utilizes the combination of AWS capabilities such as RDS snapshots, point in time restoration, and cross account replication. . The RDS Aurora service is configured to back up the production database every day on a thirty-five (35) day rolling time frame, maintain two weeks of point in time restoration capabilities, and store snapshots in a separate protected AWS region and account for worst case disaster recovery scenarios.

8. Segregation control

Data collected for different purposes must also be processed separately.

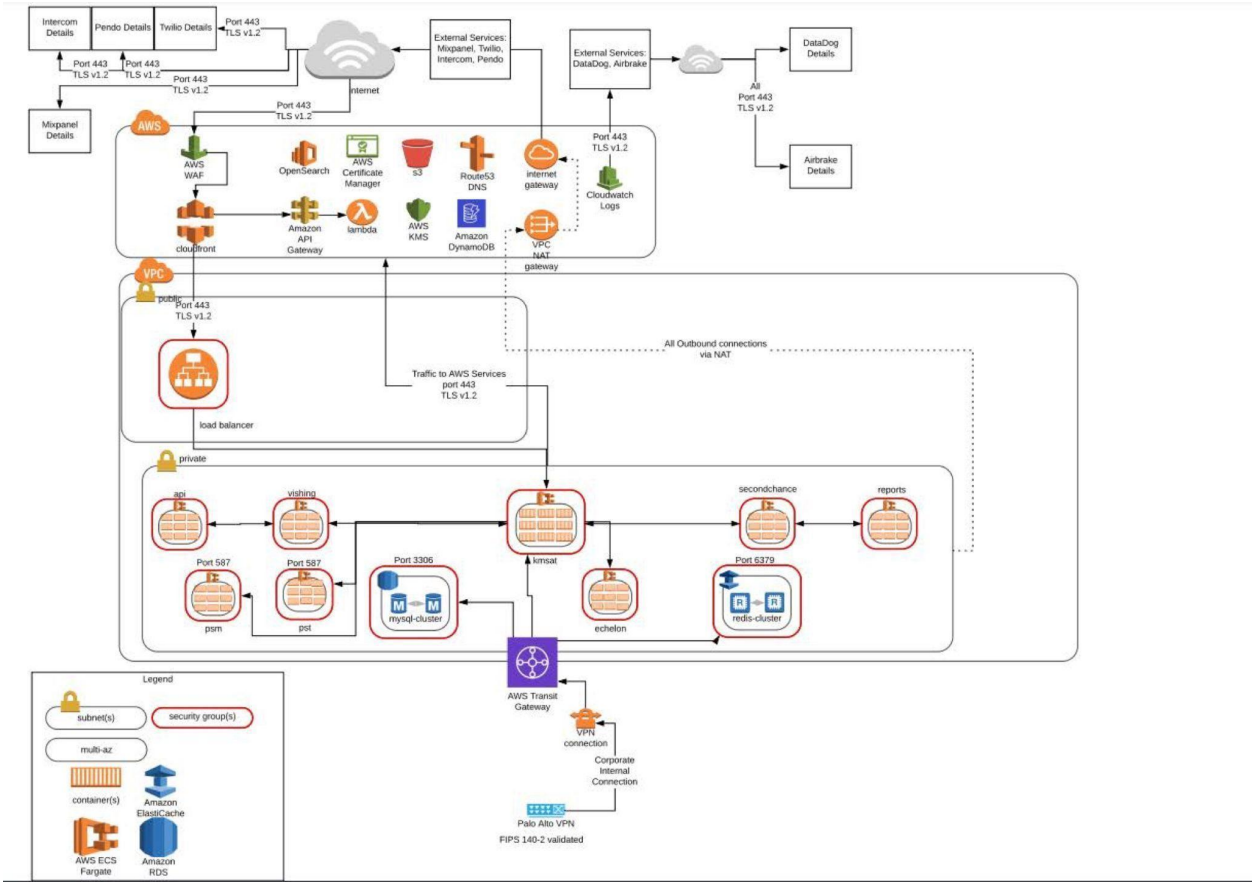
KnowBe4 operates separate production,staging, and developer on-demand environments for applications. No production or Customer Data is used in the staging or on-demand environments. The staging environment has a staging database which contains no customer information while on-demand environments have their own example databases with test data.

Customer data is segregated within the database using unique account identifiers. All data within the database can be attributed to a corresponding customer account using account ID's.

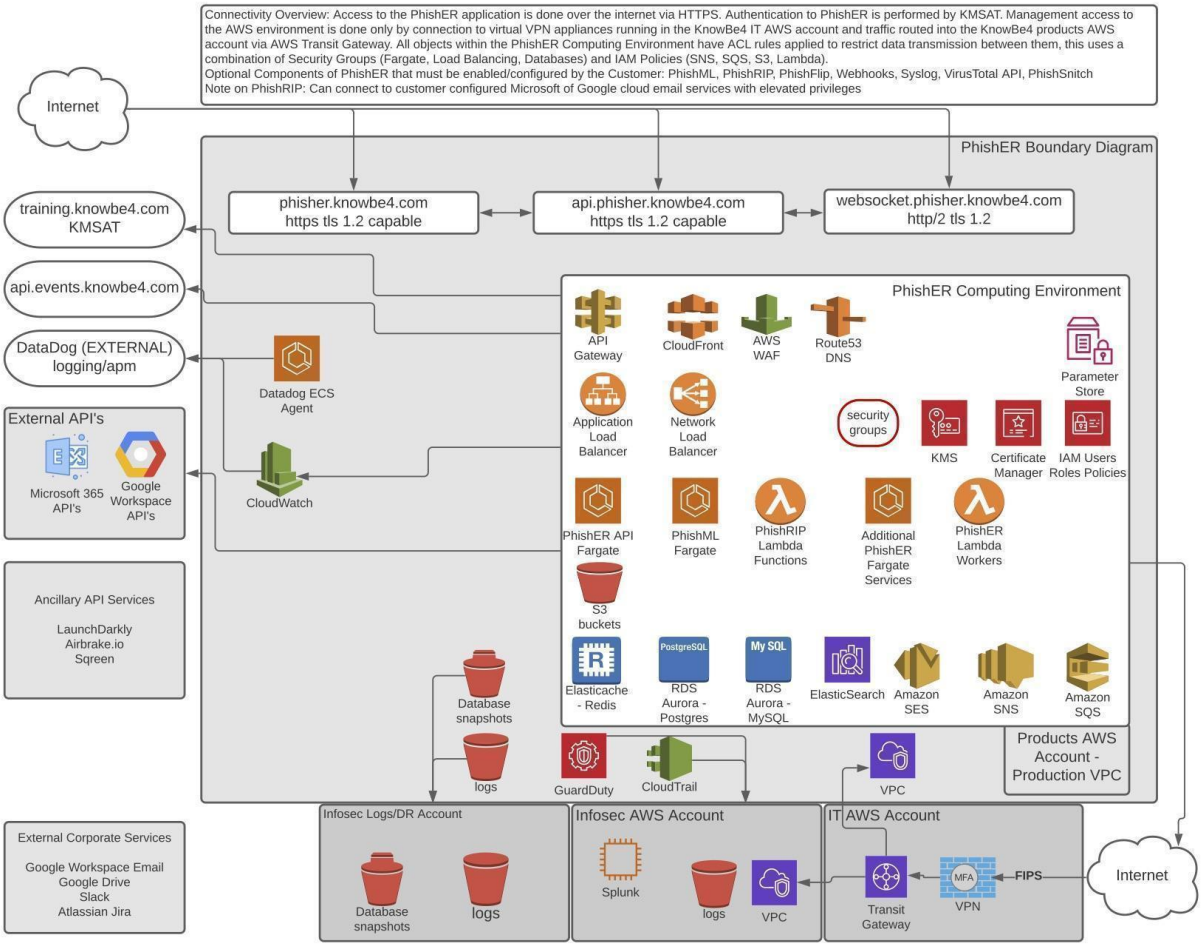
9. Application Architecture Diagram with Data Flows

A current network diagram that represents the architecture of the application and where protected information will reside.

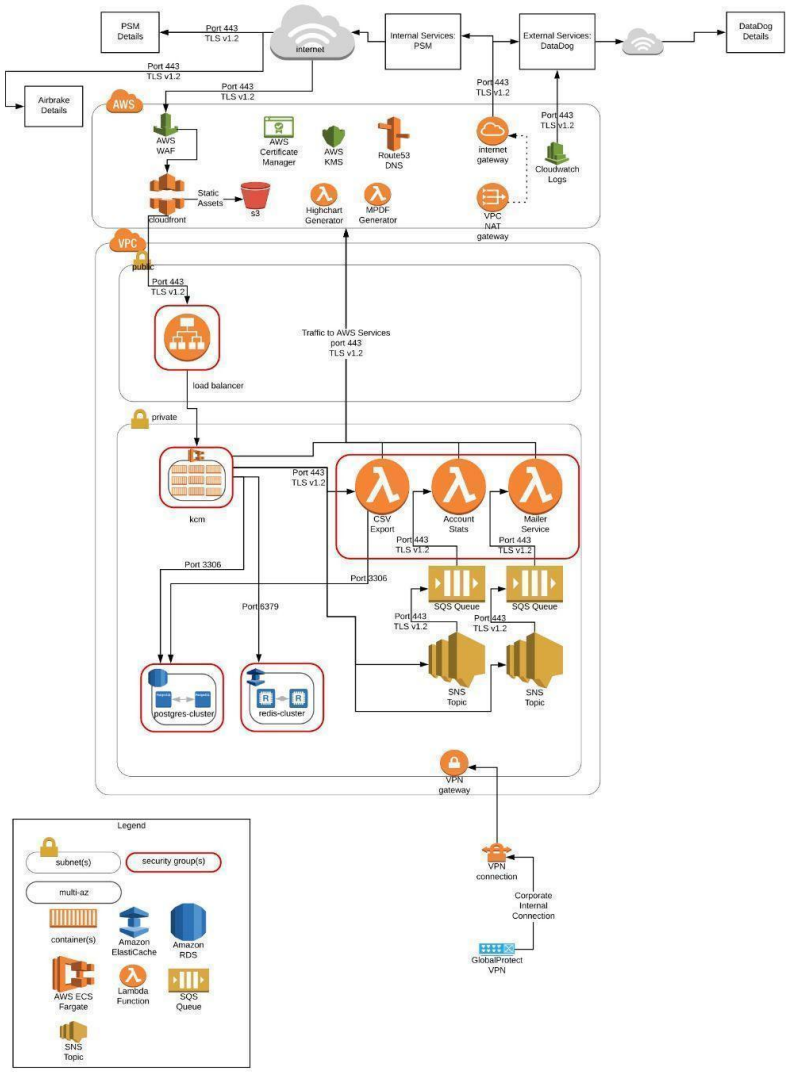
KMSAT Network Diagram



PhishER Diagram



KCM Network Diagram


PSM Details
Port 443 TLS v1.2
internet
Internal Services: PSM
External Services: DataDog
DataDog Details
Airbrake Details
Port 443 TLS v1.2
Port 443 TLS v1.2
Port 443 TLS v1.2
Port 443 TLS v1.2
AWS
AWS WAF
AWS Certificate Manager
AWS KMS
Route53 DNS
internet gateway
Cloudwatch Logs
Static Assets
cloudfront
s3
Highchart Generator
MPDF Generator
VPC NAT gateway
VPC
public
Port 443 TLS v1.2
Traffic to AWS Services port 443 TLS v1.2
load balancer
private
kcm
Port 443 TLS v1.2
CSV Export
Account Stats
Mailer Service
Port 443 TLS v1.2
Port 443 TLS v1.2
Port 3306
Port 3306
Port 6379
SQS Queue
SQS Queue
Port 443 TLS v1.2
Port 443 TLS v1.2
SNS Topic
SNS Topic
postgres-cluster
redis-cluster
VPN gateway
VPN connection
Corporate Internal Connection
GlobalProtect VPN
Legend
subnet(s)
security group(s)
multi-az
container(s)
Amazon ElastiCache
Amazon RDS
AWS ECS Fargate
Lambda Function
SQS Queue
SNS Topic

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors located at the link below.

https://support.knowbe4.com/hc/en-us/articles/1500007523981-KnowBe4-Subprocessors

Please note that this list will be strictly updated in accordance with the subprocessor requirements set forth in this document.