Effective starting: January 1st, 2025

DATA PROCESSING ADDENDUM

This Data Processing Addendum (**"DPA"**) supplements the KnowBe4 Terms of Service, or negotiated agreement in place between Customer and KnowBe4 covering Customer's use of KnowBe4's Services (the **"Agreement"**). The term "Customer" shall mean the organization entering into this DPA and shall include its Affiliates, as applicable. Unless otherwise defined in the body of this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 1 of this DPA.

1. Definitions.

"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 Data Protection Law" means all laws applicable to the Processing of Personal Data under the Agreement in the jurisdictions KnowBe4 operate.
"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.
"Data Subject" has the meaning set forth in the Applicable Data Protection Law.
"Account Data" means Personal Data relating to Customer's relationship with KnowBe4, including: (i) Users' account information (e.g., name, email address, or KnowBe4 account ID); (ii) billing and contact information of individual(s) associated with Customer's KnowBe4 account (e.g., billing address, email address, or name); (iii) Users' device and connection information (e.g., IP address); and (iv) content/description of technical support requests (excluding attachments).
"Controller" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
"Confidential Information" means all information or material disclosed by a party (the "Disclosing Party") to the other party (the "Receiving Party"), whether orally or in writing, that: (a) gives either party some competitive business advantage, gives either party an opportunity of obtaining some competitive business advantage, or the disclosure of which may be detrimental to the interests of the Disclosing Party; and (b) is either: (i) marked "Confidential," "Restricted," "Proprietary," or includes other similar markings; (ii) known by the parties to be confidential and proprietary; or (iii) from all the relevant circumstances should reasonably be assumed to be confidential and proprietary.
"**Customer Data**" means data and other information including, but not limited to, Personal Data Processed or stored through the Subscription Services by Customer or on behalf of Customer.
"Customer Personal Data" means Personal Data contained in Customer Data that KnowBe4 processes as a Processor under the Terms of Service and/or Master Service Agreement.

"Documentation" means KnowBe4 usage guidelines and standard technical documentation for the applicable Services available at support.knowbe4.com/hc/en-us or such other URL locations on KnowBe4's website as KnowBe4 may provide from time to time.
"Order" means a purchasing document or other similar document, such as a purchase order or statement of work issued by KnowBe4 ("SOW"), in connection with a purchase under the Agreement.
"Personal Data" means information about an identified or identifiable natural person, or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Applicable Data Protection Law.
"Processing" and **"Process"** and **"Processed"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
"Processor" means the legal entity which Processes Personal Data on behalf of the Controller.
"Security Incident" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data Processed by KnowBe4 and/or its Sub-processors.
"Security Measures" means KnowBe4's current technical and organizational measures as described here.
"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.
"Sub-processor" means any third party (including applicable KnowBe4 Affiliates) engaged by KnowBe4 to Process Customer Personal Data.
"Term" means the term of the Agreement.
"**Terms of Service**"/"**Master Service Agreement**" means the general use terms available at www.knowbe4.com/legal or such other URL locations on KnowBe4's website as KnowBe4 may provide from time to time, or a negotiated agreement duly executed between the parties applicable to the provision and use of the Services.
"Third-Party Products" means Software, applications, or services provided by third parties that may integrate or be used in conjunction with KnowBe4 Services.
"Threat Intelligence Data" means information collected, generated, derived, and/or analyzed by the Service that is related to malicious activities, fraud, accidental loss, human error, threat or other harm detection and analysis identified by the Service such as a third-party malicious actor's IP address, email address, name, and hashes of malware.
"Usage Data" means Personal Data, including Threat Intelligence Data, relating to or obtained in connection with the use, performance, operation, support or use of the Services, including via their connection to Third-Party Products. Usage Data may include event name (i.e. what action Users performed), event timestamps, browser information, diagnostic data, data types, file sizes, and similar information associated with data from the Services and Third-Party Products that Customer connects to the Services. For clarity, Usage Data does not include Customer Personal Data.
"Users" means individuals authorized by Customer to use the Services, which may include employees, contractors, and other representatives of Customer.

2. Scope and Term.

2.1. *Roles of the Parties.*

2.1.1. ***Customer Personal Data.*** KnowBe4 will Process Customer Personal Data as Customer's Processor in accordance with Customer's instructions as outlined in Section 3.1 (**"Customer Instructions"**).

2.1.2. ***Account Data.*** KnowBe4 will Process Account Data as a Controller for the following purposes: (i) to provide and improve the Services; (ii) to manage the Customer relationship (i.e, communicating with Customer and Users in accordance with their account preferences, responding to Customer inquiries and providing technical support, etc.); (iii) to facilitate security, fraud prevention, performance monitoring, business continuity and disaster recovery; and (iv) to carry out core business functions such as accounting, billing, and filing taxes.

2.1.3. ***Usage Data*****.** KnowBe4 will Process Usage Data as a Controller for purposes including: (i) to provide, optimize, secure, improve, and maintain the Services; (ii) to optimize user experience; and (iii) to inform KnowBe4's business strategy.

2.1.4. ***Description of the Processing.*** Details regarding the Processing of Personal Data by KnowBe4 are stated in Schedule 1 (Description of Processing).

2.2. ***Term of the DPA***. The term of this DPA coincides with the term of the Agreement and terminates upon expiration or earlier termination of the Agreement or, if later, the date on which KnowBe4 ceases all Processing of Customer Personal Data (the **"Term"**).

2.3. ***Order of Precedence.*** If there is any conflict or inconsistency among the following documents, the order of precedence is: (1) the applicable terms stated in Schedule 2 (Region-Specific Terms including any transfer provisions); (2) the main body of this DPA; and (3) the Agreement.

3. Processing of Personal Data.

3.1. ***Customer Instructions.*** When KnowBe4 processes Customer Personal Data in its capacity as a Processor on behalf of the Customer, KnowBe4 will: (i) comply with Applicable Data Protection Law; and (ii) process the Customer Personal Data as necessary to perform its obligations under the Agreement, and only in accordance with the documented lawful instructions of Customer (as set forth in the Agreement, in this DPA, or as directed by the Customer or Customer's Users through the Services), except where required otherwise by the Applicable Data Protection Law to which KnowBe4 is subject. In this case KnowBe4 shall inform the Customer of such legal requirements before processing, unless relevant Applicable Law prohibits such information on important grounds of public interest. KnowBe4 will promptly inform Customer if it becomes aware that Customer's processing instructions infringe Applicable Data Protection Law.

3.2. ***Confidentiality.*** KnowBe4 must treat Customer Personal Data as Customer's Confidential Information under the Agreement. KnowBe4 must ensure personnel authorized to Process Personal Data are bound by written or statutory obligations of confidentiality.

4. Security.

4.1. ***Security Measures.*** KnowBe4 has implemented and will maintain appropriate technical and organizational measures designed to protect the security, confidentiality, integrity and availability of Customer Data and protect against Security Incidents. Customer is responsible for configuring the Services and using features and functionalities made available by KnowBe4 to maintain appropriate security in light of the nature of Customer Data. Customer acknowledges that the Security Measures are subject to technical progress and development and that KnowBe4 may update or modify the

Security Measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Services during a Subscription Term.

4.2. ***Security Incidents.*** KnowBe4 must notify Customer without undue delay and, where feasible, no later than seventy-two (72) hours after becoming aware of a Security Incident that impacts Customer Data. KnowBe4 must make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within KnowBe4's reasonable control. Upon Customer's request and taking into account the nature of the Processing and the information available to KnowBe4, KnowBe4 must assist Customer by providing information reasonably necessary for Customer to meet its Security Incident notification obligations under Applicable Data Protection Law. KnowBe4's notification of a Security Incident is not an acknowledgment by KnowBe4 of any fault or liability. Customer shall treat any information shared during a Security Incident as Confidential Information.

5. Sub-processing.

5.1. ***General Authorization.*** By entering into this DPA, Customer provides general authorization for KnowBe4 to engage Sub-processors to Process Customer Personal Data. KnowBe4 must: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect Customer Personal Data to the standard required by Applicable Data Protection Law and to the same standard provided by this DPA; and (ii) remain liable to Customer if such Sub-processor fails to fulfill its data protection obligations with regard to the relevant Processing activities under the Agreement.

5.2. ***Notice of New Sub-processors.*** KnowBe4 maintains an up-to-date list of its Sub-processors, which contains a mechanism for Customers to subscribe to notifications of new Sub-processors. KnowBe4 will provide such notice, to those emails subscribed, at least thirty (30) days before allowing any new Sub-processor to Process Customer Personal Data (the **"Sub-processor Notice Period"**).

5.3. ***Objection to New Sub-processors.*** Customers may object to KnowBe4's appointment of a new Sub-processor during the Sub-processor Notice Period. If Customer objects, Customer, as its sole and exclusive remedy, may terminate the applicable Order for the affected Service subject to the termination clause in the Agreement.

6. Assistance and Cooperation Obligations.

6.1. ***Data Subject Rights.*** Taking into account the nature of the Processing, KnowBe4 must provide reasonable and timely assistance to Customer to enable Customer to respond to requests for exercising a data subject's rights (including rights of access, rectification, erasure, restriction, objection, and data portability) in respect to Customer Personal Data.

6.2. ***Cooperation Obligations.*** Upon Customer's reasonable request, and taking into account the nature of the Processing, KnowBe4 will provide reasonable assistance to Customer in fulfilling Customer's obligations under Applicable Data Protection Law (including data protection impact assessments and consultations with regulatory authorities, as indicated by Applicable Data Protection Law), provided that Customer cannot reasonably fulfill such obligations independently utilizing available Documentation.

6.3. ***Third Party Requests.*** Unless prohibited by Applicable Data Protection Law, KnowBe4 will promptly notify Customer of any valid, enforceable subpoena, warrant, or court order from law enforcement or public authorities compelling KnowBe4 to disclose Customer Data. In the event that KnowBe4 receives an inquiry or a request for

information from any other third party (such as a regulator or data subject) concerning the Processing of Customer Data, KnowBe4 will redirect such inquiries to Customer, and will not provide any information unless required to do so under Applicable Law.

7. Deletion and Return of Customer Data.

7.1. ***During the Term.*** During the Term, Customer and its Users may, through the features of the Services, access, retrieve or delete Customer Data.

7.2. ***Post Termination.*** Following expiration or termination of the Agreement, KnowBe4 must, in accordance with the Documentation, delete all Customer Data. Notwithstanding the foregoing, KnowBe4 may retain Customer Data: (i) as required by Applicable Data Protection Law and (ii) in accordance with its standard backup or record retention policies, provided that, in either case, KnowBe4 will maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to retained Customer Data and not further Process it except as required by Applicable Data Protection Law.

8. Audit.

8.1. ***Audit Reports.*** Upon request, KnowBe4 will supply a summary copy of its relevant audit report(s) (**"Report"**) to Customer, so Customer can verify KnowBe4's compliance with the audit standards against which it has been assessed, and this DPA. Such Report shall be deemed Confidential Information of KnowBe4. If Customer cannot reasonably verify KnowBe4's compliance with the terms of this DPA, KnowBe4 will provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its Processing of Customer Data, provided that such right may be exercised no more than once every twelve (12) months.

8.2. ***On-site Audits.*** Not more than once per calendar year during the Term of the Agreement and with at least thirty (30) days' prior written notice by Customer to KnowBe4, Customer may, at Customer's sole expense, audit KnowBe4 to verify compliance with the terms and conditions of this DPA. Such audit will be conducted only to the extent Customer cannot reasonably satisfy KnowBe4's compliance with this DPA through the exercise of its rights under Section 7.1 above, or where required by Applicable Data Protection Law or a regulatory authority. Any audit must: (i) be completed within two (2) weeks; (ii) be conducted during KnowBe4's regular business hours, with reasonable advance written notice of at least thirty (30) calendar days (unless Applicable Data Protection Law or a regulatory authority requires a shorter notice period) and accompanied by a detailed written audit plan; (iii) be performed in a manner that, in KnowBe4's reasonable judgment, does not disrupt or degrade KnowBe4's regular business operations and is done in accordance with KnowBe4's security and data protection policies; (iv) be limited to KnowBe4's facilities and personnel of KnowBe4 in scope of this Agreement; (v) be subject to reasonable confidentiality controls obligating Customer (and its authorized representatives) to keep confidential any information disclosed that, by its nature, should be confidential; (vi) occur no more than once every twelve (12) months; (vii) restrict its audit and findings to only information relevant to Customer; and (viii) be conducted by either Customer's personnel or, with KnowBe4's approval, by an independent third party mutually agreed to by the parties.

8.3. Customer may create an audit summary summarizing the findings and observations of the audit (**"Audit Summary"**). The Audit Summary is deemed to be Confidential Information of KnowBe4 and the Customer will not disclose the Audit Summaries to third parties except to Customer's legal counsel and consultants bound by obligations of

confidentiality using at least the same degree of care Customer employs in maintaining in confidence its own Confidential Information of a similar nature, but in no event less than a reasonable degree of care. The customer will disclose the results of its audit to KnowBe4 within one week after its completion. KnowBe4 will promptly respond to audit findings and, at KnowBe4's expense, discuss the findings with Customer, and if applicable, remediate and/or mitigate any critical or high-risk findings.

9. **International Provisions.** To the extent KnowBe4 Processes Personal Data protected by Applicable Data Protection Law in one of the regions listed in Schedule 2 (Region-Specific Terms), the terms specified for the applicable regions will also apply, including the provisions relevant for international transfers of Personal Data (directly or via onward transfer).

Schedule 1

Description of Personal Data Processing

Category	Description
Identity of Processor of categories of Personal Data	Customer is the Controller, and KnowBe4 is the Processor of Personal Data in Customer Personal Data as described in the DPA. For Account Data and Usage Data, KnowBe4 is the Controller.
Subject matter of Processing	Processing of Customer Personal Data, Account Data, and Usage Data as part of the Services subscribed to by Customer.
Duration of Processing	The duration of Processing of Customer Personal Data will be for the term of the Agreement. Account Data and Usage Data will be processed as long as required to provide services, for KnowBe4's legitimate business purposes, or as required by law.
Hosting Location	As specified in the Agreement or relevant Orders. If not specified, processing will occur across at least 2 availability zones offered by the relevant third-party Sub-Processor.
Nature of Processing	Customer Personal Data is Processed by KnowBe4 and its Sub-Processors to provide the Services and related Services (including computing, storage, support and such other services) as determined by Customer and Users under, and described in, the DPA and Agreement.

Purpose of Processing	For Customer Personal Data: As instructed by Customer. For Account Data and Usage Data: For the purposes as specified in Section 2 of this DPA.
Type of Personal Data	Customer Personal Data may include Personal, Special Category and confidential Personal Data as determined by Customer. Account Data and Usage Data do not include sensitive data.
Categories of Data Subjects	Users of the Services as determined by Customer.
Categories of data	Customer Personal Data: As determined by Customer, may include email contents and any data uploaded by Users. Account Data: Organizational account information, billing and contact information, device and connection information. Usage Data: Data relating to use of Services, including event data, timestamps, browser information, diagnostic data.

Schedule 2

Region-Specific Terms and Definitions

Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this Schedule will have the meanings given to them in Section 1 of this Schedule.

1. Definitions.

Where Personal Data is subject to the laws of one the following regions, the definition of **"Applicable Data Protection Law"** includes:

- **Australia:** the Australian Privacy Act;
- **Brazil:** the Brazilian Lei Geral de Proteção de Dados (General Personal Data Protection Act);
- **Canada:** the Canadian Personal Information Protection and Electronic Documents Act;
- **Europe:** (i) the Regulation 2016/679 of the European Parliament and of the Council 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, or GDPR) and (ii) the EU e-Privacy Directive (Directive 2002/58/EC) as amended, superseded or replaced from time to time (**"EU Data Protection Law"**);
- **Japan:** the Japanese Act on the Protection of Personal Information;
- **Singapore:** the Singapore Personal Data Protection Act;
- **South Korea:** the South Korean Personal Information Protection Act (**"PIPA"**) and the Enforcement Decrees of PIPA;

- **Switzerland:** the Swiss Federal Act on Data Protection and its implementing regulations as amended, superseded, or replaced from time to time (**"Swiss FADP"**);
- **The United Kingdom:** the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 as amended, superseded or replaced from time to time (**"UK Data Protection Law"**); and
- **The United States:** all state laws relating to the protection and Processing of Personal Data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations ("**CCPA"**), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act (**"US State Privacy Laws"**).

"Deidentified Data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, a data subject.

"Data Privacy Framework" means the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework self-certification program operated by the US Department of Commerce.

"Europe" includes, for the purposes of this DPA, the Member States of the European Union and European Economic Area.

"EU SCCs" means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended, superseded, or replaced from time to time.

"Service Provider" has the same meaning as given in the CCPA.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, as amended, superseded or replaced from time to time.

2. EU, United Kingdom and Switzerland.

2.1. ***Customer Instructions.*** In addition to Section 3.1 (Customer Instructions) of the DPA above, KnowBe4 will Process Customer Personal Data only on documented instructions from Customer, including with regard to transfers of such Customer Personal Data to a third country or an international organization, unless required to do so by Applicable Data Protection Law to which KnowBe4 is subject; in such a case, KnowBe4 shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. KnowBe4 will promptly inform Customer if it becomes aware that Customer's Processing instructions infringe Applicable Data Protection Law.

2.2. ***European Transfers.*** Where Personal Data protected by the EU Data Protection Law is transferred, either directly or via onward transfer, to a country outside of Europe that is not subject to an adequacy decision, the following applies:

2.2.1. The EU SCCs are hereby incorporated into this DPA by reference as follows:

2.2.1.1. Customer is the "data exporter" and KnowBe4 is the "data importer".

2.2.1.2. Module One (Controller to Controller) applies where KnowBe4 is Processing Account Data or Usage Data.

2.2.1.3. Module Two (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and KnowBe4 is Processing Customer Personal data as a Processor.

2.2.1.4. Module Three (Processor to Processor) applies where Customer is a Processor of Customer Personal Data and KnowBe4 is Processing Customer Personal Data as another Processor.

2.2.1.5. By entering into this DPA, each party is deemed to have signed the EU SCCs as of the commencement date of the Agreement.

2.2.2. For each Module, where applicable:

2.2.2.1. In Clause 7, the optional docking clause does not apply.

2.2.2.2. In Clause 9, Option 2 applies, and the time period for prior notice of Sub-processor changes is stated in Section 4 (Sub-processing) of this DPA.

2.2.2.3. In Clause 11, the optional language does not apply.

2.2.2.4. In Clause 17, Option 1 applies, and the EU SCCs are governed by Irish law.

2.2.2.5. In Clause 18(b), disputes will be resolved before the courts of Ireland.

2.2.2.6. The Appendix of EU SCCs is populated as follows:

- The information required for Annex I(A) is located in the Agreement and/or relevant Orders.
- The information required for Annex I(B) is located in Schedule 1 (Description of Processing) of this DPA.
- The competent supervisory authority in Annex I(C) will be determined in accordance with the Applicable Data Protection Law; and
- The information required for Annex II is located here.

2.3. ***Swiss Transfers.*** Where Personal Data protected by the Swiss FADP is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the EU SCCs apply as stated in in Section 2.2 (European Transfers) above with the following modifications:

2.3.1. All references in the EU SCCs to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP, and references to specific Articles of "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of the Swiss FADP; all references to the EU Data Protection Law in this DPA will be interpreted as references to the FADP.

2.3.2. In Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

2.3.3. In Clause 17, the EU SCCs are governed by the laws of Switzerland.

2.3.4. In Clause 18(b), disputes will be resolved before the courts of Switzerland.

2.3.5. All references to Member State will be interpreted to include Switzerland and Data Subjects in Switzerland are not excluded from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).

2.4. ***United Kingdom Transfers.*** Where Personal Data protected by the UK Data Protection Law is transferred, either directly or via onward transfer, to a country outside of the United Kingdom that is not subject to an adequacy decision, the following applies:

2.4.1. The EU SCCs apply as set forth in Section 2.2 (European Transfers) above with the following modifications:

2.4.1.1. Each party shall be deemed to have signed the UK Addendum.

2.4.1.2. For Table 1 of the UK Addendum, the parties' key contact information is located in the Agreement and/or relevant Orders.

2.4.1.3. For Table 2 of the UK Addendum, the relevant information about the version of the EU SCCs, modules, and selected clauses which this UK Addendum is appended to is located above in Section 2.2 (European Transfers) of this Schedule.

2.4.1.4. For Table 3 of the UK Addendum:

- The information required for Annex 1A is located in the Agreement and/or relevant Orders.
- The Information required for Annex 1B is located in Schedule 1 (Description of Processing) of this DPA.
- The information required for Annex II is located here.
- The information required for Annex III is located in Section 5 (Sub-processing) of this DPA.

2.4.1.5. In Table 4 of the UK Addendum, both the data importer and data exporter may end the UK Addendum.

2.5. ***Data Privacy Framework.*** KnowBe4 participates in and certifies compliance with the Data Privacy Framework. As required by the Data Privacy Framework, KnowBe4 (i) provides at least the same level of privacy protection as is required by the Data Privacy Framework Principles; (ii) will notify Customer if KnowBe4 makes a determination it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework Principles, and (iii) will, upon written notice, take reasonable and appropriate steps to remediate any unauthorized Processing of Personal Data.

3. United States of America. The following terms apply where KnowBe4 Processes Personal Data subject to the US State Privacy Laws:

3.1. To the extent Customer Personal Data includes personal information protected under US State Privacy Laws that KnowBe4 Processes as a Service Provider or Processor, on behalf of Customer, KnowBe4 will Process such Customer Personal Data in accordance with the US State Privacy Laws, including by complying with applicable sections of the US State Privacy Laws and providing the same level of privacy protection as required by US State Privacy Laws, and in accordance with Customer's written instructions, as necessary for the limited and specified purposes identified in Section 2.1.1 (Customer Personal Data) and Schedule 1 (Description of Processing) of this DPA. KnowBe4 will not:

3.1.1. retain, use, disclose or otherwise Process such Customer Personal Data for a commercial purpose other than for the limited and specified purposes identified in this DPA, the Agreement, and/or any related Order, or as otherwise permitted under US State Privacy Laws;

3.1.2. "sell" or “share” such Customer Personal Data within the meaning of the US State Privacy Laws; and

3.1.3. retain, use, disclose or otherwise Process such Customer Personal Data outside the direct business relationship with Customer and not combine such Customer Personal Data with personal information that it receives from other sources, except as permitted under US State Privacy Laws.

3.2. KnowBe4 must inform Customer if it determines that it can no longer meet its obligations under US State Privacy Laws within the timeframe specified by such laws, in which case Customer may take reasonable and appropriate steps to prevent, stop, or remediate any unauthorized Processing of such Customer Personal Data.

3.3. To the extent Customer discloses or otherwise makes available Deidentified Data to KnowBe4 or to the extent KnowBe4 creates Deidentified Data from Customer Personal Data, in each case in its capacity as a Service Provider, KnowBe4 will:

3.3.1. adopt reasonable measures to prevent such Deidentified Data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

3.3.2. publicly commit to maintain and use such Deidentified Data in a de-identified form and to not attempt to re-identify the Deidentified Data, except that KnowBe4 may attempt to re-identify such data solely for the purpose of determining whether its de-identification processes are compliant with the US State Privacy Laws; and

3.3.3. before sharing Deidentified Data with any other party, including Sub-processors, contractors, or any other persons (**"Recipients"**), contractually obligate any such Recipients to comply with all requirements of this Section 3.3 (including imposing this requirement on any further Recipients).

4. South Korea. The following terms apply where KnowBe4 Processes Personal Data subject to the South Korean Privacy Laws:

4.1. Customer agrees that it has provided notice and obtained all consents and rights necessary under Applicable Data Protection Law for KnowBe4 to Process Account Data and Usage Data pursuant to the Agreement (including this DPA).

4.2. To the extent Customer discloses or otherwise makes available Deidentified Data to KnowBe4, KnowBe4 will:

4.2.1. maintain and use such Deidentified Data in a de-identified form and not attempt to re-identify the Deidentified Data; and

4.2.2. before sharing Deidentified Data with any other party, including Sub-processors, contractors, or any other persons (**"Recipients"**), contractually obligate any such Recipients to comply with all requirements of this Section 4.2 (including imposing this requirement on any further Recipients).