

DATA PROCESSING ADDENDUM

This Data Processing Addendum (“DPA”) is incorporated into and forms part of the AuditBoard Subscription Agreement between AuditBoard, Inc. (“AuditBoard”), and Customer with respect to use of the Services (the “Agreement”). This DPA sets out the requirements for AuditBoard’s processing of Personal Data on behalf of Customer for the purposes of providing the Services.

This DPA is effective on the date of the Agreement. Each of AuditBoard and Customer may be referred to as a “party” and together as “parties”.

1. DEFINITIONS

“CCPA” means the California Consumer Privacy Act, Cal. Civ. Code Section 1798.100 et seq. and its implementing regulations as may be amended from time to time.

“Controller” means the entity which, along or jointly with others, determines the purpose and means of Processing of Personal Data, including as applicable any ‘business’ as that term is defined in the CCPA.

“Processor” means the entity which Processes Personal Data on behalf of the Data Controller, including as applicable any ‘service provider’ as that term is defined in the CCPA.

“Data Protection Laws” means all data protection and privacy laws applicable to the Processing of Personal Data under this DPA, including local, state, national and/or foreign laws, treaties, and/or regulations, including without limitation the GDPR, and implementations of the GDPR into national law, and CCPA, in each case as may be amended or superseded from time to time.

“Data Subject” means the Person to who the Personal Data relates.

“Data Subject Request” means a request from or on behalf of a data subject to exercise any rights in relation to their Personal Data under Data Protection Laws.

“GDPR” means either or both the General Data Protection Regulation (EU) 2016/679 (“EU GDPR”) and the EU GDPR as it forms part of the United Kingdom (“UK”) law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (“UK GDPR”) as the context may require.

“Personal Data” means all Customer Data that relates to an identified or identifiable natural person.

“Processing” or “Process” means any operation or set of operations performed on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

“Restricted Country” means: (i) where the EU GDPR applies, a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a country outside the UK which is not based on adequacy regulations pursuant to Section 17A of the UK Data Protection Act 2018; and (iii) where the Swiss Federal Act on Data Protection applies, a country outside Switzerland which has not been recognized to provide an adequate level of protection by the Federal Data Protection and Information Commissioner.

“Restricted Transfer” means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area (“EEA”) to a Restricted Country; (ii) where the UK GDPR applies, a transfer of Personal Data from the UK to a Restricted Country; and (iii) where the Swiss Federal Act on Data Protection applies, a transfer of Personal Data from Switzerland to a Restricted Country.

“Security Policy” means AuditBoard’s Security Policy currently located at: <https://www.auditboard.com/enterprise-agreements/>. AuditBoard may update the Security Policy from time to time provided that such updates do not result in a material reduction of the security of the Services.

“Standard Contractual Clauses” means (i) where the EU GDPR applies, the clauses annexed to the European Commission’s Implementing Decision 2021/914 of 4 June 2021 for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (“EU SCCs”); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR (“UK SCCs”).

“Subprocessor” means an AuditBoard Affiliate or third-party entity engaged by AuditBoard or a AuditBoard Affiliate as a Data Processor under this DPA.

“Subprocessor List” means the subprocessor list identifying the Subprocessors that are authorized to Process Personal Data, accessible through AuditBoard’s website (currently located at <https://www.auditboard.com/subprocessors/>).

“UK” means the United Kingdom.

Any capitalised terms which are not defined in this DPA are as defined in the Agreement.

2. ROLES & COMPLIANCE WITH DATA PROTECTION LAWS

- 2.1 For the purposes of this DPA, Customer is the controller of Personal Data, and AuditBoard is the processor of Personal Data except when Customer acts as a Data Processor of Personal Data, in which case AuditBoard is a Subprocessor. The Parties shall comply with all applicable Data Protection Laws.

2.2 AuditBoard will only process Personal Data per Customer's documented instructions. Customer instructs AuditBoard to Process Personal Data to provide the Service in accordance with the Agreement (including this DPA) and as further specified via Customer's use of the Service. AuditBoard will notify Customer (unless prohibited by applicable law) if it is required under applicable law to process Personal Data other than pursuant to Customer's instructions. Further, AuditBoard will, as soon as reasonably practicable upon becoming aware, inform the Customer if, in AuditBoard's reasonable opinion, any instructions provided by the Customer infringe Data Protection Laws. To the extent the CCPA applies to Personal Data, AuditBoard will not (i) Sell or Share Personal Data, nor (ii) retain, use or disclose Personal Data for any purpose other than to provide the Services in accordance with the Agreement; (iii) retain, use, or disclose Personal Data outside the direct business relationship between AuditBoard and Customer; (iv) combine Personal Data with personal information that AuditBoard has received from another AuditBoard customer, except as permitted under the CCPA. AuditBoard will notify Customer if AuditBoard determines that AuditBoard can no longer comply with our obligations as a Service Provider. Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information that is protected under the CCPA. The Term "Sell", "Share", "Service Provider", and "Personal Information" shall have the meaning set forth in the CCPA. "Personal Information" shall refer to any Personal Data that constitutes Personal Information under the CCPA.

3. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

3.1 AuditBoard will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data as outlined in Security Policy.

3.2 AuditBoard shall require screening of its personnel who may have access to Personal Data and shall require such personnel (i) to Process Personal Data in accordance with Customer's instructions as set forth in this DPA, (ii) to receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data; and (iii) to be subject to confidentiality obligations which shall survive the termination of employment. AuditBoard will take reasonable steps to ensure that any persons whom it authorizes to access the Personal Data are under obligations of confidentiality which shall survive the termination of employment.

4. DATA SECURITY INCIDENTS

4.1 **Data Security Incidents.** AuditBoard will notify Customer of any Data Security Incident as outlined in section 6 of the Agreement for Personal Data breaches.

5. FURTHER ASSISTANCE

5.1 **Assistance with Data Subject Requests.** AuditBoard will, in a manner consistent with the functionality of the Service and AuditBoard's role as a Processor, provide reasonable support to Customer to enable Customer to respond to Data Subject Requests.

5.2 **Handling of Subject Requests.** For the avoidance of doubt, Customer is responsible for responding to Data Subject Requests. If AuditBoard receives a Data Subject Request or other complaint from a Data Subject regarding the Processing of Personal Data, AuditBoard will promptly forward such request or complaint to Customer, provided the Data Subject has given sufficient information for AuditBoard to identify the Customer.

5.3 **Data Protection Impact Assessments and Prior Consultations.** Customer agrees that, to the extent applicable, AuditBoard's then-current SOC 2 audit reports (or comparable industry-standard successor reports) and/or AuditBoard's ISO certifications will be used to carry out Customer's data protection impact assessments and prior consultations, and AuditBoard shall make such reports available to Customer. To the extent Customer requires additional assistance to meet its obligations under applicable Data Protection Law to carry out a data protection impact assessment and prior consultation with the competent supervisory authority related to Customer's use of the Service, AuditBoard will, taking into account the nature of Processing and the information available to AuditBoard, provide such reasonable assistance to Customer, at the Customer's cost to be agreed beforehand.

6. SUBPROCESSORS

6.1 Customer hereby agrees and provides a general authorization that AuditBoard and AuditBoard's Affiliates may engage Subprocessors. AuditBoard will make available to Customer a Subprocessor List and provide Customer with a mechanism to obtain notice of any updates to the Subprocessor List. AuditBoard will provide notice to Customer at least 30 days prior to authorizing any new Subprocessor to process Personal Data by updating the Subprocessor List.

6.2 AuditBoard will consider any of Customer's reasonable objections to a new Subprocessor within 30 days of Customer's notification of such new Subprocessor pursuant to Section 6.1 to the extent that Customer is located in the EEA, the UK, or Switzerland or where otherwise required by Data Protection Laws applicable to Customer. If Customer has a reasonable objection to any new or replacement Subprocessor and the parties cannot agree a resolution within thirty (30) days of the objection, Customer's sole and exclusive remedy is to terminate the relevant portion(s) of the Service within those thirty (30) days, by providing written notice to AuditBoard. Upon any termination by Customer pursuant to this Section, AuditBoard shall refund Customer any prepaid fees for the terminated portion(s) of the Service that were to be provided after the effective date of termination.

6.3 AuditBoard will enter into a written contract with each Subprocessor which imposes on such Subprocessor terms no less protective of Personal Data than those imposed on AuditBoard in this DPA. AuditBoard shall be liable to Customer for any breach by such Subprocessor of any of obligation set forth herein to the extent as if the acts or omissions were performed by AuditBoard.

7. INTERNATIONAL TRANSFERS

7.1 Customer agrees that its use of the Services may involve the transfer of Personal Data to, and processing of Personal Data in, locations outside of the EEA, UK or Switzerland from time to time, such as for purposes of providing support to Customer.

7.2 **Processor-to-Processor SCCs.** Where AuditBoard is located within the EEA, UK or Switzerland AuditBoard has implemented the Standard Contractual Clauses for any Restricted Transfers of Personal Data from AuditBoard (as "data exporter") to Subprocessors (as "data importers").

7.3 **Controller-to-Processor SCCs.** Where AuditBoard is located in a Restricted Country, the Standard Contractual Clauses will apply to any Restricted Transfers from Customer (as "data exporter") to AuditBoard (as "data importer") as follows:

7.4 **EU Personal Data.** In relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module 2 applies unless the Customer is a Processor in which case Module 3 applies; (ii) in Clause 7, the optional docking clause will apply; (iii) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes will be in accordance with the notification process set out in Section 6.1 of this DPA; (iv) in Clause 11, the optional redress language will not apply; (v) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by the law specified in the MSA, provided that law is an EEA Member State law recognizing third party beneficiary rights, otherwise, the laws of Ireland apply; (vi) in Clause 18(b), disputes shall be resolved before the courts specified in the MSA, provided these courts are located in an EU Member State, otherwise those courts shall be the courts of Ireland; (vii) Annex I of the Standard Contractual Clauses shall be deemed completed with the information set out in Annex I to this DPA; and (viii) Annex II of the Standard Contractual Clauses shall be deemed completed with the information set out in the Security Policy.

7.5 **UK Personal Data.** In relation to Personal Data that is protected by the UK GDPR ("UK Personal Data"), the UK SCCs will apply as follows:

(i) The EU SCCs, completed as set out in Section 7.4 above, shall also apply to transfers of such UK Personal Data; and (ii) The UK Addendum shall be deemed executed between the transferring Customer and AuditBoard, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such UK Personal Data. Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out in Section 7.4 above, and the options "Exporter" and "Importer" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the effective date of this DPA.

7.6 **Swiss Personal Data.** In relation to Personal Data that is protected by the Swiss Federal Act on Data Protection, the EU SCCs will apply amended and adapted as follows:

(i) the Swiss Federal Data Protection and Information Commissioner is the exclusive supervisory authority; (ii) the term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18; and (iii) references to the GDPR in the EU SCCs shall also include the reference to the equivalent provisions of the Swiss Federal Act on Data Protection (as amended or replaced).

7.7 **Clarifications.** The Standard Contractual Clauses will be subject to the following clarifications:

(i) AuditBoard will allow Customer to conduct audits as described in the Standard Contractual Clauses in accordance with Section 8 of this DPA. (ii) Customer consents to AuditBoard appointing Subprocessors in accordance with Section 6 of this DPA, and Customer may exercise its right to object to Subprocessors under the Standard Contractual Clauses in the manner set out in Section 6.2. (iii) AuditBoard shall return and delete Customer's data in accordance with Section 9 of this DPA. (iv) Customer agrees that any assistance that AuditBoard provides to Customer under the Standard Contractual Clauses shall be in accordance with Section 5 of this DPA. (v) Nothing in this Section 7.7 of this DPA varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses. If any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

8. AUDIT AND RECORDS

8.1 AuditBoard will, subject to the confidentiality terms in the Agreement, provide Customer in writing such information in AuditBoard's possession or control as may be necessary to demonstrate compliance with its obligations under this DPA. Customer agrees that, to the extent applicable, AuditBoard's then-current Audit Reports will be used to satisfy any audit or inspection requests by or on behalf of Customer. Customer will not exercise the audit rights specified in this Section 8.1 more than once in any twelve (12) calendar month period. Any additional audits or inspections beyond those described in this Section 8.1 will be at Customer's cost, to be agreed in advance. To the extent Customer reasonably determines that the Audit Reports are not sufficient to demonstrate compliance or to respond to a regulatory audit, AuditBoard will allow Customer or an independent auditor appointed by Customer to conduct an audit, subject to the following: (i) Customer and AuditBoard will mutually agree upon the scope, timing, duration, and control and evidence requirements; (ii) Customer is responsible for all costs and fees related to such audit and will reimburse any services performed by AuditBoard at AuditBoard's then current rates; (iii) such audit occurs no more than once annually; (iv) to the extent the audit is conducted by a third-party audit firm, (a) the third-party audit firm is not a competitor of AuditBoard and (b) Customer, has, prior to such audit, entered into an agreement with such third-party audit firm containing confidentiality terms no less protective than the confidentiality terms set forth in the Agreement; and (v) to the extent the audit is conducted by a regulator having jurisdiction over Customer, the regulator is subject to a duty of confidentiality in relation to the findings of that audit (whether arising as a matter of law or by Customer having, prior to such audit, entered into an agreement with the regulator) such duty being no less protective than the confidentiality terms set forth in the Agreement.

9. DELETION OR RETURN OF DATA

9.1 Upon termination of this DPA, AuditBoard will return or delete the Personal Data in accordance with the relevant provisions of the Agreement. Notwithstanding the foregoing, AuditBoard may retain Personal Data beyond termination solely if, and for so long as, such Personal Data must be retained in order to comply with applicable law.

10. GENERAL

10.1 **Conflicts.** This DPA is without prejudice to the rights and obligations of the parties under the Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms (including definitions) of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data. This DPA sets out all of the terms that have been agreed between the parties in relation to the subjects covered by it. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA.

10.2 **Customer Affiliate Enforcement.** Customer's Affiliates may enforce the terms of this DPA directly against AuditBoard, subject to the following provisions:

(i) Customer will bring any legal action, suit, claim or proceeding which that Affiliate would otherwise have if it were a party to the Agreement (each an "Affiliate Claim") directly against AuditBoard on behalf of such Affiliate, except where the Data Protection Laws to which the relevant Affiliate is subject require that the Affiliate itself bring or be party to such Affiliate Claim; and

(ii) for the purpose of any Affiliate Claim brought directly against AuditBoard by Customer on behalf of such Affiliate in accordance with this Section, any losses suffered by the relevant Affiliate may be deemed to be losses suffered by Customer.

10.3 **Termination.** The term of this DPA will end simultaneously and automatically at the later of (i) the termination of the Agreement or, (ii) when all Personal Data is deleted from AuditBoard's systems.

10.4 **Remedies.** Customer's remedies (including those of its Affiliates) with respect to any breach by AuditBoard, its Affiliates and Subprocessors of the applicable terms of this DPA, and the overall aggregate liability of AuditBoard and its Affiliates arising out of, or in connection with the Agreement (including this DPA) will be subject to any aggregate limitation of liability that has been agreed between the parties under the Agreement.

10.5 **Miscellaneous.** The section headings contained in this DPA are for reference purposes only and shall not in any way affect the meaning or interpretation of this DPA.

ANNEX I

Description of Processing

1 A. LIST OF PARTIES

Data exporter(s):

Data exporter: Customer.
Contact details: As set out in the Agreement.
Activities relevant to the data transferred under these Clauses: Use of Audit Board's cloud applications.
Signature and date: By entering into the Agreement, data exporter is deemed to have signed these Standard Contractual Clauses incorporated herein as of the effective date of the Agreement.
Role: The data exporter's role is set forth in the DPA.

Data importer(s):

Data Importer: AuditBoard, Inc.
Address: 12900 Park Plaza Dr, Suite 200, Cerritos, CA 90703
Contact person's name, position and contact details: AuditBoard Legal and Privacy Team, legal@auditboard.com
Activities relevant to the data transferred under these Clauses: Provide and support enterprise cloud applications, including audit and risk management.
Signature and date: By entering into the Agreement, data importer is deemed to have signed these Standard Contractual Clauses incorporated herein as of the effective date of the Agreement.
Role (controller/processor): Processor

2 B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

- Employee's or contact persons of Customer.

Categories of personal data transferred:

- Name and contact information (including work address; work telephone numbers; mobile telephone numbers; web address; IP addresses; instant messenger; work email address); business title; company.

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):

- Continuous.

Nature of the processing:

- The nature and purposes of the processing is the collection, storage, duplication, deletion, and disclosure of Personal Data pursuant to providing the Services to Customer (including AuditBoard's provision of its enterprise cloud applications, including SoxHub and audit management).

Purpose(s) of the data transfer and further processing:

- *Provide and support enterprise cloud applications.*

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

- *Personal Data will be retained for the duration of the Agreement.*

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

- *The subject matter, nature and duration of the data importer's transfers to sub-processors are as set out within the Subprocessor List (currently located at <https://www.auditboard.com/subprocessors/>).*

3 C. COMPETENT SUPERVISORY AUTHORITY

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

- *The supervisory authority is the Data Protection Commission of Ireland.*

ANNEX II

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

AuditBoard has implemented and maintains appropriate technical and organisational measures to ensure a level of security commensurate to the risk to the Personal Information as outlined in the Security Policy. Such measures include taking appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, and the risks for the rights and freedoms of natural persons.